Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de
Ingeniería de Sistemas e Informática

Modelo de seguridad de la información basado en la Iso/IEC 27001:2013 para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín

Jean Carlo Zacarias Villafranca

Huancayo, 2017

Tesis para optar el Título Profesional de
Ingeniero de Sistemas e Informática

AGRADECIMIENTOS

En primer lugar, a Dios por darme salud y pasión para vivir y por permitirme concluir satisfactoriamente el presente trabajo de investigación, a mis padres, familiares y novia por su apoyo incondicional y desinteresado.

A mi asesor Ing. Edson Raúl Lazo Álvarez, gracias a su paciencia y experiencia que ha impartido sus enseñanzas con excelencia, motivándonos a obtener nuevos conocimientos y un panorama holístico del tema elegido para poder desarrollar la presente tesis.

Al Sr. gral. Jesús Moisés Ríos Vivanco, Jefe de la Región Policial Junín (2016); Sr. gral. PNP José Luís Cueva Velarde, Director de la VI Macrorregión Junín-Pasco-Huancavelica de la PNP; Sr. crnl. PNP Manuel Tafur Torres Jefe del Estado Mayor de la Región Policial Junín y SS. PNP Moisés Vidal Huamán Pari Jefe de la Oficina de Planeamiento Administrativo del Estado Mayor de la Región Policial Junín y a mis colegas de la Central de Operaciones Policiales de la Región Policial Junín, quienes me brindaron las facilidades necesarias para el desarrollo del presente proyecto de investigación.

A mis colegas, amigos y compañeros de estudio por compartir sus experiencias y conocimientos durante el desarrollo de la investigación.

A mis padres:

Carmen y Percy, quienes con su dedicación y perseverancia han sido siempre ejemplo para mí, pues motivan todos mis esfuerzos.

A mi novia:

María, gracias por confiar en mí y ser sostén de mis decisiones.

A mi amiga:

Nilda, agradezco tus buenos consejos y tu apoyo sincero e incondicional.

Jean Carlo

ÍNDICE

CAPÍTULO IV
PLANEAMIENTO Y EJECUCIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO V
RESULTADOS Y DISCUSIÓN

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

La información es un activo esencial y decisivo para la viabilidad de una organización y al estar disponible en ambientes cada vez más interconectados y en distintos formatos, está expuesta a amenazas y vulnerabilidades; por lo que, se decidió implementar un modelo de seguridad de la información en la Central de Operaciones Policiales de la Región Policial Junín. La investigación tuvo como objeto determinar la influencia de un modelo de seguridad de la información basado en la norma ISO/IEC 27001:2013 para mitigar los riesgos a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín. La investigación desarrollada fue de tipo aplicada a nivel explicativo. Para el estudio se consideró como muestra a la totalidad del personal policial que labora en la Central de Operaciones Policiales de la Región Policial Junín. La hipótesis de la investigación fue: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye significativamente en mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín. En conclusión, la investigación logró demostrar que la implementación de un modelo de seguridad de la información basada en la norma ISO/IEC 27001:2013 influye positivamente en la mitigación de los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, ya que el nivel de concientización y percepción del personal policial sobre mitigación de riesgos preimplementación fue de 24% y postimplementación fue de 99%, lo que significa un aumento de 75% en el nivel de concientización y percepción del personal policial sobre mitigación de riesgos de los activos de información.

Palabras clave: información, modelo de seguridad de la información, norma ISO/IEC 27001:2013, riesgos de los activos de información, amenazas y vulnerabilidades.

ABSTRACT

Information is an essential and decisive asset for the viability of an organization and being available in increasingly interconnected environments and in different formats is exposed to threats and vulnerabilities; So it was decided to implement an information security model in the Police Operations Center of the Junín Police Region. The research was aimed at determining the influence of an information security model based on ISO / IEC 27001: 2013 to mitigate risks to information assets in the Police Operations Center of the Junín Police Region. The research developed was of an applied type at an explanatory level. For the study, all the police personnel working in the Police Operations Center of the Junín Police Region were considered as a sample. The research hypothesis was: The establishment of a model for information security based on ISO 27001 significantly influences the mitigation of the risks of information assets in the Police Operations Center of the Junín Police Region. In conclusion, the research demonstrated that the implementation of an information security model based on ISO / IEC 27001: 2013 has a positive influence on the mitigation of the risks of information assets in the Police Operations Center of the Police Region Junín, since the level of awareness and perception of police personnel on pre-implementation risk mitigation was 24% and post-implementation was 99%, which means a 75% increase in the level of awareness and perception on risk mitigation Of the information assets.

Key words: Information, Information security model, ISO/IEC 27001:2013, risks of information assets, threats and vulnerabilities.

INTRODUCCIÓN

A diario observamos en los medios de comunicación, fuente abierta y redes sociales casos de fuga de información policial - la misma que se ha acrecentado dado el uso ma de los dispositivos móviles y aplicaciones de mensajería instantánea - que en el trámite interno de documentación policial han sido clasificados como confidencial, secreto o reservado; por ende no deben ser de conocimiento público, pese a ello son revelados en muchas ocasiones por el propio personal que integra la Policía Nacional del Perú, dando a conocer datos sensibles, fotografías y filmaciones de personas involucradas en actos ilícitos (intervenidos o detenidos) y hasta documentos oficiales, los que podrían constituirse en delito en el fuero militar, policial y penal, infracción al régimen disciplinario de la Policía Nacional del Perú y a la ley de protección de datos personales, no siendo ajenos a dichos incidentes la Central de Operaciones Policiales de la Región Policial Junín, ya que la información que gestiona es su principal activo.

Por lo que, la presente investigación se enfocó principalmente en identificar los riesgos de los activos de información y concientizar al personal policial a cargo del manejo de la información para mitigar dichos riesgos, habiéndoles consultado (antes y después) su percepción sobre incidencias de amenazas y vulnerabilidades con el objetivo de determinar la influencia de un modelo de seguridad de la información basado en la ISO/IEC 27001:2013 para mitigar los riesgos a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Asimismo, el presente trabajo presenta los siguientes capítulos:

En el Capítulo I, se detallan la fundamentación y formulación del problema, también se dan a conocer los objetivos general y específicos que trazaron la investigación para su desarrollo. Dicho capítulo finaliza manifestando la justificación de la importancia de la investigación desarrollada, basada en la hipótesis de investigación y la identificación y descripción de variables que dio inicio al presente estudio.

En el capítulo II, se detalla un marco teórico de los antecedentes del problema, en el cual se describen los hechos más resaltantes encontrados a nivel nacional e internacional; asimismo, se dan a conocer las bases teóricas relacionadas al tema de

investigación. El capítulo finaliza manifestando la definición de términos básicos, metodologías y tecnologías utilizadas en el desarrollo de la presente investigación.

El capítulo III definido por la metodología, se inicia con la definición de tipificación y método de investigación y diseño utilizado en el trabajo de investigación. La población y muestra establecida en el estudio como también las técnicas e instrumentos utilizados en la recolección de datos en la presente investigación.

En el capítulo IV, se detalla el planeamiento, ejecución y procedimientos que se deben tener en cuenta al implementar un sistema de gestión de seguridad de la información, definiendo los entregables realizados, así como el análisis de riesgos de los activos de información utilizando la metodología *Magerit* y el instrumento *Pilar* que nos permitieron identificar las amenazas y vulnerabilidades más frecuentes. Al finalizar el capítulo se desarrolló el modelo de seguridad de la información aplicando políticas de seguridad de la información basadas en la norma ISO/IEC 27001:2013, procediendo con la capacitación y prueba respectiva.

El capítulo V definido por el análisis de los resultados y discusión, se detallan los resultados obtenidos de la investigación, se nombra la aceptación o rechazo de la hipótesis de investigación. Al finalizar el capítulo se realizó la discusión de resultados dando realce a las variables y el contraste con los fundamentos teóricos y los resultados experimentales obtenidos. Para finalizar el informe de investigación se describen las conclusiones y recomendaciones a fin de realizar futuras investigaciones relacionadas con el tema.

CAPÍTULO I

PLANTEAMIENTO DEL ESTUDIO

1.1 Fundamentación y formulación del problema

El presente trabajo de investigación se desarrolló en la Central de Operaciones Policiales de Región Policial Junín con sede en la ciudad de Huancayo, en el periodo de noviembre del 2016 a febrero del 2017.

1.1.1 Fundamentación del problema

La Central de Operaciones Policiales de Región Policial Junín es el órgano de apoyo cuya función es de enlace entre el Jefe de la Región Policial Junín y los comisarios, jefes o encargados de departamentos especializados de la Región Policial Junín, encargado de recopilar, centralizar, dar a conocer y en ocasiones sugerir las acciones inmediatas para la toma de decisiones por parte del Sr. general PNP Jefe de la Región Policial Junín ante situaciones de crisis, emergencias y/o conflictos sociales; además, recibe disposiciones de los órganos superiores del sistema policial como Dirección General PNP, Dirección Nacional de Operaciones Policiales PNP y otros y se encarga de procesar y automatizar, organizar y centralizar la información operativa (producción policial) a nivel región Junín, en forma permanente para coadyuvar las acciones a optimizar la operatoria policial y la toma de decisiones contando con la información actualizada y de forma automática desde cualquier lugar conforme a los niveles de acceso y seguridad correspondiente.

En dicho contexto, al manipular digital y físicamente documentación con información de carácter reservado, confidencial y secreto requiere implementar controles en las aplicaciones y sistemas de información que utiliza.

1.1.2 Formulación del problema

Problema general

Por lo antes descrito, en el presente estudio de investigación se desea determinar cuál es la influencia de un modelo de seguridad de la información basado en la norma ISO 27001 para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Problemas específicos

Asimismo, al observarse dicha problemática surgieron las siguientes interrogantes:

- ¿Cuál es la influencia de un modelo de seguridad de la información basado en la ISO 27001 para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín?
- ¿Cuál es la influencia de un modelo de seguridad de la información basado en la ISO 27001 para mitigar las vulnerabilidades de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín?

1.2 Objetivos

1.2.1 Objetivo general

Determinar la influencia de un modelo de seguridad de la información basado en la ISO/IEC 27001:2013 para mitigar los riesgos a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

1.2.2 Objetivos específicos

a. Establecer un modelo de seguridad de la información y determinar su influencia para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.
b. Establecer un modelo de seguridad de la información y determinar su influencia para mitigar la vulnerabilidad de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

1.3 Justificación

Por medio de la presente investigación se pretende hacer uso de las normas orientadas a la seguridad de los activos de información, para solucionar un problema latente en la Central de Operaciones Policiales de la Región Policial Junín, orientada a identificar los niveles de riesgo de los activos de información, mejorar la seguridad en el uso de las aplicaciones y sistemas de almacenamiento de información que se utiliza y mitigar las fugas y pérdidas de información, partiendo desde la concientización del personal policial comprometido, ya que en muchas ocasiones se constata que información e imágenes de propiedad de la PNP circulan deliberadamente por medios de comunicación, fuente abierta y redes sociales; por lo que, podemos instituir o cimentar un modelo de seguridad de la información basado en la norma ISO 27001:2013.

Además, reitero que el presente estudio de investigación podría servir de apoyo a futuras investigaciones relacionadas con la identificación de riesgos de los activos de información policial y mejorar los niveles de seguridad en las aplicaciones y sistemas de información que utiliza la Policía Nacional del Perú.

Finalmente, la presente investigación orienta su justificación a los ámbitos tecnológico y científico, conforme al siguiente detalle:

Tecnológico: porque se proyecta a ser un referente para la seguridad de los activos de la información en la Policía Nacional del Perú, ya que se empleará normas y tecnologías orientadas exclusivamente a dicho campo de la informática, siendo muy probable obtener un modelo de seguridad de la información basado en la ISO/IEC 27001:2013 que pueda ser instituido en la Policía Nacional del Perú.

Científico: porque podría servir de referencia y apoyo a futuras investigaciones relacionadas con la identificación de riesgos de los activos de información, para así mejorar los niveles de seguridad en el uso de las aplicaciones y sistemas de información que utiliza la Policía Nacional del Perú.

1.4 Fundamentación y formulación de las hipótesis

1.4.1 Hipótesis general

El establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye significativamente en mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Hipótesis nula

Ho: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 no influye en la mitigación de los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín

Hipótesis alternativa

H1: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye positivamente en la mitigación de los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

1.4.2 Hipótesis específicas

a. El establecimiento de un modelo de seguridad de la información influye directamente en mitigar las amenazas de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.
b. El establecimiento de un modelo de seguridad de la información influye directamente en mitigar las vulnerabilidades de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

1.5 Identificación y descripción de las variables

A continuación, se describen las variables de estudio y tabla ilustrativa:

- **Variable X**: ISO 27001:2013, Sistema de Gestión de Seguridad de la Información (independiente)
  Dimensiones: Sistema de Gestión de Seguridad de la Información (confidencialidad, integridad y disponibilidad).
- **Variable Y**: riesgos de los activos de información (dependiente)
  Dimensiones: amenazas y vulnerabilidades.

Tabla 1. Descripción de variables

VARIABLES	DIMENSIONES	DESCRIPCIÓN
Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 (Gómez Fernández, Luís y Andrés Álvarez, Ana)	Sistema de Gestión de Seguridad de la Información (confidencialidad, integridad y disponibilidad)	Variable independiente
Riesgo de los activos de información (Instituto Nacional de Ciberseguridad del Gobierno de España)	Amenazas	Variable dependiente
	Vulnerabilidades	

Fuente: Elaboración Propia

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes del problema

2.1.1 Antecedentes nacionales

El presente trabajo de investigación se desarrolló a partir de las siguientes investigaciones previas de carácter nacional:

- **Según la autora Zully Isabel Justino Salinas, con el tema de investigación titulado: "Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013", de la Pontificia Universidad Católica del Perú. Año 2015. Sostiene que:**

  "… pese a que, en la última década, algunas empresas han puesto énfasis al tema de seguridad de información, muchas otras han tenido problemas con respecto a este tema; es así como los riesgos que enfrenta una organización se materializan, tales como fraudes, fuga y pérdida de información, exposición de información confidencial, entre otros. Según Isaca, a nivel global, el 22% de las empresas estudiadas habían sido víctimas de ataques a su seguridad y el 21% enfrentaba problemas con dispositivos; en otras palabras, una de cada cuatro empresas sufre problemas de seguridad de información. Además, en Latinoamérica, se encontró que tres de cada diez empresas, experimentaron una brecha de seguridad y el 16% ha enfrentado problemas de seguridad en dispositivos móviles. [Isaca, 2012a] En este entorno, se debe saber que, para solucionar

estos problemas, cada organización tendrá sus propias necesidades y/o requerimientos de seguridad". (Justino Salinas, 2015)

- **Según los autores David Aurelio Fernández Peñaloza y Oscar Alexis Pacheco Vargas, con el tema de investigación titulado: "Mejora de seguridad de información en la Comandancia de Operaciones Guardacostas basada en la norma técnica peruana NTP-ISO/IEC 27001:2008", de la Universidad San Martín de Porres de Lima-Perú. Año 2014. Sostienen que:**

  "… Los resultados obtenidos fueron minimizar los riesgos, amenazas y vulnerabilidades de los activos de información como también el compromiso del personal de la Comandancia con respecto a la seguridad de información.

La conclusión es que nuestro modelo aplicado, ha permitido desarrollar el Plan de Sistema de Gestión de Seguridad de la información de la Comandancia basado en la norma NTP-ISO/IEC 27001:2008". (Fernández Peñaloza, 2014)

2.1.2 Antecedentes Internacionales

El presente trabajo de investigación se desarrolló considerando los siguientes trabajos y antecedentes internacionales:

- **Según los autores Juan David Aguirre Cardona y Catalina Aristizabal Betancourt, con el tema de investigación titulado: "Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda", de la Universidad Tecnológica de Pereira de Colombia. Año 2013. Sostienen que:**

  "… es fundamental para la empresa la implementación del sistema de gestión de seguridad de la información porque aparte de salvaguardar el activo más importante, se puede tener a la mano la asesoría necesaria y el apoyo continuo que fundamenta el ciclo PHVA 1.

  El sistema de gestión de seguridad de la información contribuye a poder estar a la altura de las grandes organizaciones que buscan en las certificaciones de este tipo, una de las mayores ventajas competitivas para lanzarse al mercado ya explorado y a los mercados que aún se encuentran disponibles, los cuales por el crecimiento global se han tornado exigentes para grandes contrataciones con el Estado, con grandes superficies para

realizar transacciones electrónicas y acogerse a ellas mediante distintos canales de pago para la sostenibilidad y manejo de los clientes a nivel nacional e internacional". (Aguirre Cardona, 2013)

- **Según el autor Gustavo Pallas Mega, con el tema de investigación titulado: "Metodología de implantación de un SGSI en un grupo empresarial jerárquico", de la Universidad de la República de Uruguay. Año 2009. Sostiene que:**

  "… se requiere de un sistema de gestión de seguridad de la información (SGSI) y un accionar proactivo. Si consideramos un grupo empresarial, donde dos o más empresas se integran verticalmente, el desafío de gestionar la seguridad de una manera conveniente es aún mayor.

  En este trabajo, se analizan diferentes enfoques de estos estándares, con el fin de proponer una metodología de implementación, gestión y mejora de un SGSI en un grupo empresarial jerárquico. Se presentan además diferentes alternativas estratégicas y se discute sobre su conveniencia o no. Se analizan diferentes métodos conocidos de análisis y gestión de riesgos." (Pallas Mega, 2009)

2.2 Base teórica

Para la presente investigación tomé en cuenta las siguientes definiciones de los autores que se detallan a continuación:

2.2.1 Definición de información

"La información es un activo esencial y es decisiva para la viabilidad de una organización. Adopta diferentes formas: impresa, escrita en papel, digital, transmitida por correo, mostrada en videos o hablada en conversaciones.

Debido a que está disponible en ambientes cada vez más interconectados, está expuesta a amenazas y vulnerabilidades." (Luis Gómez Fernández, 2009)

"La información es un activo que, como otros activos importantes del negocio, tiene valor para una organización y por lo tanto necesita ser protegido adecuadamente" (27001 ACADEMY)

2.2.2 Definición de un Sistema de Gestión de Seguridad de la Información

"Es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización." (27001 ACADEMY)

"Para proteger la información de una manera coherente y eficaz es necesario implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema es una parte del sistema global de gestión, basado en un análisis de los riesgos del negocio, que permite asegurar la información frente a la pérdida de:

- Confidencialidad: sólo accederá a la información quien se encuentre autorizado.
- Integridad: la información será exacta y completa.
- Disponibilidad: los usuarios autorizados tendrán acceso a la información cuando lo requieran." (Luis Gómez Fernández, 2009)

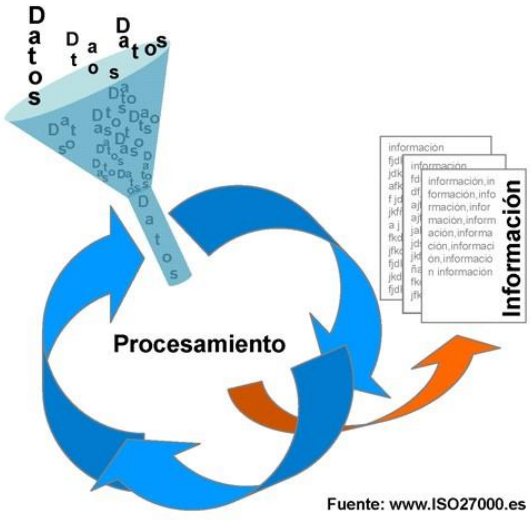


Figura 1. Procesamiento de datos a información

Fuente: (27001 ACADEMY)

2.2.3 El ciclo de mejora continua

"Para establecer y gestionar un sistema de gestión de la seguridad de la información se utiliza el ciclo PDCA (conocido también como ciclo *Deming*), tradicional en los sistemas de gestión de la calidad.

El ciclo PDCA es un concepto ideado originalmente por *Shewhart*, pero adaptado a lo largo del tiempo por algunos de los más sobresalientes personajes del mundo de la calidad. Esta metodología ha demostrado su aplicabilidad y ha permitido establecer la mejora continua en organizaciones de todas clases.

El modelo PDCA o "Planificar-Hacer-Verificar-Actuar" (*Plan-Do-Check-Act*, de sus siglas en inglés), tiene una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización:

- *Plan*: esta fase se corresponde con establecer el SGSI. Se planifica y diseña el programa, sistematizando las políticas a aplicar en la organización.
- *Do*: es la fase en la que se implementa y pone en funcionamiento el SGSI.
- *Check*: esta fase es la de monitorización y revisión del SGSI.
- *Act*: Es la fase en la que se mantiene y mejora el SGSI, decidiendo y efectuando las acciones preventivas y correctivas necesarias para rectificar." (Luis Gómez Fernández, 2009)

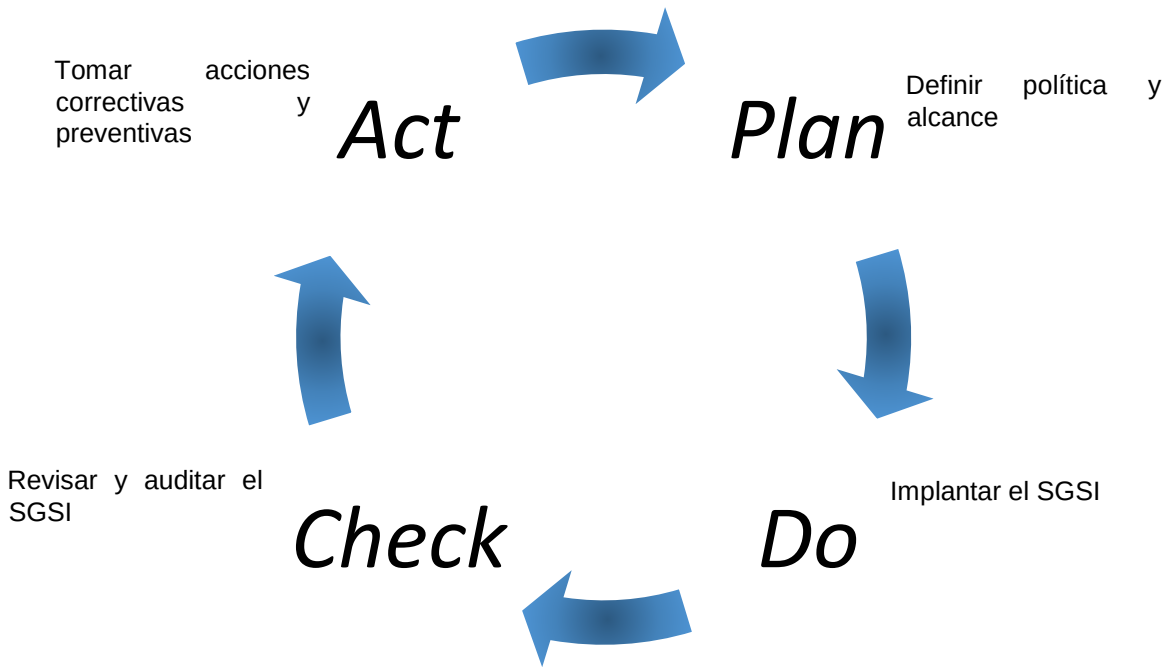


Figura 2. Ciclo PDCA de mejora continua

Fuente: (Luis Gómez Fernández, 2009)

2.2.4 La Norma UNE-ISO/IEC 27001

2.2.4.1 Origen de la norma

"ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial.

Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo." (27001 ACADEMY)

2.2.4.2 Objeto y campo de aplicación de la norma

"Esta norma específica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en

cuenta los riesgos empresariales generales de la organización.” (27001 ACADEMY)

2.2.4.3 Aspectos básicos de la Norma ISO/IEC 27001

La ISO/IEC 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO), describe cómo gestionar la seguridad de la información adecuada en una empresa. ISO/IEC 27001 puede ser implementada en cualquier tipo de organización, a su vez puede ser, con o sin fines de lucro, privada o pública, pequeña o grande. Esta norma está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.

2.2.4.4 Como funciona ISO/IEC 27001.

Su eje central es proteger la confidencialidad, la integridad y disponibilidad de la información en una determinada empresa. Para dicha actividad se encarga de investigar y revisar cuáles son los potenciales problemas que podrían afectar la información (la evaluación de riesgos) y luego define lo que es necesario hacer para evitar que estos problemas se produzcan o se terminen manifestando (mitigación o tratamiento del riesgo). Por lo tanto, la filosofía principal de la norma ISO/IEC 27001 está basada en la gestión de riesgos: investigándolos y luego tratándolos sistemáticamente.

En cuanto a las medidas de seguridad (o controles) que se van a implementar estos se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero los utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Figura 3. Estructura de la ISO 27001

Fuente: (27001 ACADEMY)

2.2.4.5 Proceso de implementación de la ISO/IEC 27001. Enfoque de las seis fases o pasos esenciales del proceso.

Dentro del proceso de implementación de la ISO/IEC 27001, podemos mencionar el siguiente enfoque para su posible implementación:

- Definir una política de seguridad de información
- Definir el alcance del modelo
- Efectuar un análisis y evaluación del riesgo
- Definir opciones del tratamiento del riesgo
- Seleccionar controles a implantar
- Preparar un enunciado de aplicabilidad

2.2.4.6 Beneficios que brinda ISO/IEC 27001

Existen cuatro ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información, las que a su vez son las siguientes:

- Cumplir con los requerimientos legales
- Obtener una ventaja comercial
- Menores costos
- Una mejor organización

2.2.4.7 Donde interviene ISO/IEC 27001

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

Figura 4. Alcance de la ISO/IEC 27001

Fuente: (27001 ACADEMY)

2.2.5 Gestión de riesgos

"Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

El objetivo a proteger es la misión de la organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

Disponibilidad o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio.

La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una organización.

Confidencialidad o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados.
La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que nos acerquen a la percepción de los usuarios de los sistemas de información:

Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos.
Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

Trazabilidad: aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.” (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

2.2.5.1 Aspectos básicos de la metodología *Magerit*

Esta metodología hace referencia al análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión en las organizaciones respectivamente.

2.2.5.2 Estructura de la metodología *Magerit*

Esta metodología tiene una estructura adecuada la cual se describirá a continuación:

El capítulo 2, presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

El capítulo 3, concreta los pasos y formaliza las actividades de análisis de los riesgos.

El capítulo 4, describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.

El capítulo 5, se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

El capítulo 6, formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.

El capítulo 7, se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

El capítulo 8, se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

2.2.5.3 Objetivos de *Magerit*

Entre los distintos objetivos que persigue la siguiente metodología tenemos a los siguientes objetivos directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

2.2.5.4 Fundamentos de *Magerit*

Puntualmente esta metodología se basa fuertemente en analizar el impacto que puede tener para la empresa la violación de su seguridad, busca la identificación de las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Lo interesante de esta metodología, es que presenta una guía completa y con detalles paso a paso de cómo llevar a cabo el análisis de riesgos.

2.2.5.5 Ventajas de la metodología *Magerit*

La metodología *Magerit* permite saber cuánto valor está en juego en las organizaciones y por ende ayuda a protegerlo. Asimismo, conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con esta metodología, se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

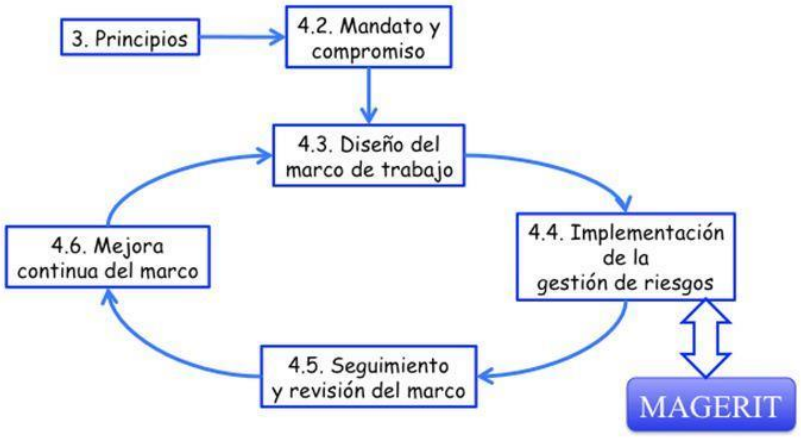


Figura 5. Diseño de Gestión de Riesgos de Magerit

Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

1.3 Definición de términos básicos

El presente trabajo lo desarrollé utilizando siglas y términos incluidos en las variables, los que procedo a describirlos a continuación:

- ISO: (*International Standarization Organization*) es la entidad internacional encargada de favorecer normas de fabricación, comercio y comunicación en todo el mundo. Con sede en Ginebra, es una federación de organismos nacionales entre los que se incluyen Aenor en España, DIN en Alemania y Afnor en Francia. (27001 ACADEMY)
- ISO 27001: es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. (27001 ACADEMY)
- NTC-ISO/IEC 27001:2013: estándar para la seguridad de la información. *Information technology - Security techniques - Information security management systems – Requirements*; aprobado y publicado como estándar internacional en octubre de 2013 por *International Organization for Standardization* y por la comisión *International Electrotechnical Commission*. (27001 ACADEMY)
- SGSI: Sistema de Gestión de Seguridad de la Información. (27001 ACADEMY)
- Sistema de Gestión de Seguridad de la Información: es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. (27001 ACADEMY)

- **Confidencialidad**: garantiza que la información sea accesible sólo para aquellas personas autorizadas. En el Manual de Documentación Policial está relacionado con los aspectos disciplinarios del personal o irregularidades administrativas que por su gravedad deben ser conocidos únicamente por el remitente y el destinatario, o por las personas encargadas de opinar o resolver sobre el particular. (27001 ACADEMY)
- **Integridad**: garantiza la exactitud y totalidad de la información y los métodos de procesamiento. (27001 ACADEMY)
- **Disponibilidad**: garantiza que los usuarios autorizados tengan siempre acceso a la información y a los recursos relacionados con ella. (27001 ACADEMY)
- **Secreto**: referidos a los asuntos de extrema importancia o cuyo conocimiento indiscriminado podría generar problemas que afecten a la Seguridad Nacional. (General, 2016)
- **Reservado**: aquellos relacionados con la prevención y represión de la criminalidad en el país, cuya revelación pueden entorpecerlas. (General, 2016)
- **Auditabilidad**: permitir la reconstrucción, revisión y análisis de la secuencia de eventos. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Identificación**: verificación de una persona o cosa; reconocimiento. (Mataix Lorda, 1999)
- **Autenticación**: proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, que se tiene o una combinación de todas.
- **Autorización**: lo que se permite cuando se ha otorgado acceso.
- **No repudio**: no se puede negar un evento o una transacción. (27001 ACADEMY)
- **Control de acceso**: limitar el acceso autorizado solo a entidades autenticadas. (27001 ACADEMY)
- **Métricas de seguridad, monitoreo**: medición de actividades de seguridad
- **Estrategia**: los pasos que se requieren para alcanzar un objetivo (27001 ACADEMY)
- **Gerencia**: vigilar las actividades para garantizar que se alcancen los objetivos.
- **Gobierno TI**: consiste en una estructura de relaciones y procesos destinados a dirigir y controlar la empresa, con la finalidad de alcanzar sus objetivos y añadir valor mientras se equilibran los riesgos y el retorno sobre TI y sus procesos. (27001 ACADEMY)

- **Política de seguridad**: es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma. (27001 ACADEMY)
- **Estrategias de seguridad**: es un patrón frente al cual una compañía toma sus decisiones de protección de la información con base en sus objetivos y propósito.
- **Ingeniería de seguridad**: usa todo tipo de ciencias para desarrollar los procesos y diseños en cuanto a las características de seguridad, controles y sistemas de seguridad. (27001 ACADEMY)
- **Riesgo**: la explotación de una vulnerabilidad por parte de una amenaza. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Exposiciones**: áreas que son vulnerables a un impacto por parte de una amenaza
- **Vulnerabilidades**: deficiencias que pueden ser explotadas por amenazas. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Amenaza**: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir daño -material o inmaterial- sobre los elementos -activos, recursos- de un sistema. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Ataque**: es una amenaza que se convirtió en realidad, es decir cuando un evento se realizó. No dice nada si fue o no exitoso el evento. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Autenticidad**: la legitimidad y credibilidad de una persona, servicio o elemento debe ser comprobable. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Elementos de Información**: también activos o recursos de una institución que requieren protección, para evitar su pérdida, modificación o el uso inadecuado de su contenido, para impedir daños para la institución y las personas que salen en la información. Se distingue y divide en tres grupos, a) Datos e información, b) Sistemas e infraestructura y c) Personal. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Activos de información**: es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información

como pueden ser las Bases de Datos con usuarios, contraseñas, números de cuentas, etc. (27001 ACADEMY)

- **Gestión de riesgo**: método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Está compuesta por cuatro fases: 1) Análisis, 2) Clasificación, 3) Reducción y 4) Control de Riesgo. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Integridad**: datos son completos, no modificados y todos los cambios son reproducibles (se conoce el autor y el momento del cambio). (27001 ACADEMY)
- **Seguridad informática**: procesos, actividades, mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad. (27001 ACADEMY)
- **Vulnerabilidad**: son la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Riesgo residual**: el riesgo que permanece después de que se han implementado contra medidas y controles. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Impacto**: los resultados y consecuencias de que se materialice un riesgo. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Criticidad**: La importancia que tiene un recurso para el negocio. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Sensibilidad**: el nivel de impacto que tendría una divulgación no autorizada. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Análisis de impacto al negocio**: evaluar los resultados y las consecuencias de la inestabilidad. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Controles**: cualquier acción o proceso que se utiliza para mitigar el riesgo (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

- **Contra medidas**: cualquier acción o proceso que reduce la vulnerabilidad. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Políticas**: declaración de alto nivel sobre la intención y la dirección de la gerencia. (Luis Gómez Fernández, 2009)
- **Normas**: establecer los límites permisibles de acciones y procesos para cumplir con las políticas.
- **Ataques**: tipos y naturaleza de inestabilidad en la seguridad. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Clasificación de datos:** el proceso de determinar la sensibilidad y criticidad de la información.
- ***Magerit***: implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- **Análisis de riesgos**: es el uso sistemático de la información disponible para determinar la frecuencia con la que determinados eventos se pueden producir y la magnitud de sus consecuencias. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)
- ***Telegram***: aplicación de mensajería instantánea.

CAPÍTULO III
METODOLOGÍA

3.1 Métodos y alcance de la investigación

El presente proyecto de investigación está contextualizado de la siguiente manera:

Método universal: método científico.

Tipo de investigación: aplicada.

Nivel de investigación: explicativa.

Por lo tanto, a partir de un marco teórico de referencia, se realiza un análisis de los modelos teóricos existentes a fin de poder diseñar un modelo de seguridad a la medida de las necesidades identificadas en la Central de Operaciones Policiales de la Región Policial Junín.

3.2 Diseño de la investigación

Para el presente proyecto de investigación se ha establecido un diseño de investigación: experimental - cuasi experimental.

Conforme al siguiente diseño:

X

G: O1 → O2

Tabla 2. Modelo de diseño cuasi experimental

Grupo	Asignación	Preprueba	Estímulo	Postprueba	Hipótesis
GE		O1	X	O2	o1<o2

1ro. Medición previa de la variable dependiente a ser estudiada (pretest).

2do. Aplicación de la variable independiente o experimental X a los sujetos Y.

3ro. Una nueva medición de la variable dependiente en los sujetos Y (postest).

Donde:

GE: grupo experimental

O1: primera observación, pretest

X: aplicación o tratamiento de la variable independiente.

O2: segunda observación, postest

Hipótesis: Si **O1<O2** se acepta la hipótesis.

Si **O1>O2** se rechaza la hipótesis y se acepta la hipótesis nula.

3.3 Población y muestra

3.3.1 Universo

En el presente trabajo de investigación se consideró a la totalidad de efectivos policiales integrantes de la Región Policial Junín.

3.3.2 Población

Es el conjunto bien definido de unidades de observación con características comunes y perceptibles a quienes se desea beneficiar. En el presente trabajo de investigación se consideró a la totalidad de efectivos policiales integrantes de la Central de Operaciones Policiales de la Región Policial Junín.

3.3.3 Muestra

Para la presente investigación se ha considerado a todos los individuos de mi población, por lo que, no se ha realizado un cálculo poblacional.

Según Hernández y Fernández 1991: al observar que la población es muy pequeña se tomarán a los 32 trabajadores de la subunidad policial.

La selección de la muestra será en base a un muestreo no probabilístico, de tipo intencional o por conveniencia; que para el caso la muestra será el total de la población.

3.4 Técnicas e instrumentos de recolección de datos

3.4.1 Técnicas

Las técnicas e instrumentos que se utilizaron en el presente proyecto de investigación son las técnicas que a continuación se detallan:

- Ficha de observación y verificación

- Encuestas
- Análisis de riesgos

3.4.2 Instrumentos

- Fichas bibliográficas: el investigador registra las referencias bibliográficas.
- Cuestionario de preguntas: el investigador realizará visitas a la Ceopol para evaluar la percepción y adopción de las políticas de seguridad.
- Guía de observación de incidencias por fugas y pérdidas de información: el investigador obtiene directamente los datos de la realidad, sin intermediarios ni distorsiones de la información.
- Análisis de riesgo *Magerit*: el investigador utilizará el software *Pilar* para determinar los niveles de riesgo utilizando la metodología *Magerit*.

CAPÍTULO IV
PLANEAMIENTO Y EJECUCIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para el problema planteado e implementación del Sistema de Gestión de la Seguridad de la Información se tomó en cuenta lo siguiente:

4.1 Norma ISO/IEC 27001:2013

4.1.1 Entregables definidos por ISO/IEC 27001

Los diferentes entregables que se tomaron en cuenta con la metodología de la Norma ISO/IEC 27001:2013, para mitigar los riesgos de los activos de información de la Central de Operaciones Policiales de la Región Policial Junín, son los siguientes:

- **Entregable 1: procedimiento para el control y registro de documentos**
  Objetivo del entregable: establecer los procedimientos, principios y normas para la elaboración y control de los documentos y registros asociados al Sistema de Gestión de Seguridad de la Información de la Central de Operaciones Policiales de la Región Policial Junín.
- **Entregable 2: plan del proyecto**
  Objetivo del entregable: el objetivo del plan del proyecto es definir claramente el propósito del proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), los documentos que se redactarán, los plazos, las funciones y responsables del proyecto.
- **Entregable 3: procedimiento para la identificación de requisitos**
  Objetivo del entregable: el objetivo del presente documento es definir el proceso de identificación de las partes interesadas, de los requisitos

legales, normativos, contractuales y de otra índole relacionados con la seguridad de la información y con la continuidad del negocio, como también los responsables de su cumplimiento.

- **Entregable 4: documento sobre el alcance del SGSI**
  Objetivo del entregable: el objetivo de este documento es definir claramente los límites del Sistema de Gestión de Seguridad de la Información (SGSI) de la Central de Operaciones Policiales de la Región Policial Junín.
  Los usuarios de este documento son los efectivos policiales de la Central de Operaciones Policiales de la Región Policial Junín.
- **Entregable 5: política de seguridad de la información**
  Objetivo del entregable: la presente política de alto nivel tiene como propósito definir el objetivo, dirección, principios, disposiciones y reglas básicas para la gestión de la seguridad de la información en la Central de Operaciones Policiales de la Región Policial Junín.
- **Entregable 6: declaración de aplicabilidad**
  Objetivo del entregable: el objetivo del presente documento es definir los controles adecuados a implementarse en la Central de Operaciones Policiales de la Región Policial Junín, además de identificar los objetivos, forma de implementación, aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.
- **Entregable 7: plan de tratamiento del riesgo**
  Objetivo del entregable: se detallan las actividades necesarias e imprescindibles para conseguir los objetivos del SGSI.
- **Entregable 8: plan de capacitación y concienciación**
  Objetivo del entregable: establecer normas y procedimientos para impartir conocimientos y procedimientos para la aplicación adecuada del Sistema de Gestión de Seguridad de la Información, dirigido al personal policial de la Central de Operaciones Policiales y Oficina Regional de Inteligencia de la Región Policial Junín.

4.2 Metodología *Magerit*

"Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, actualizada el 2012 en su versión 3".

(Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en la Central de Operaciones Policiales de la Región Policial Junín y definir el nivel aceptable de riesgo según la Norma ISO/IEC 27001:2013.

Esta metodología contempla diferentes actividades enmarcadas a los activos que una organización posee para el tratamiento de la información, su estructura está dada por la Norma ISO 27002.

4.2.1 Herramienta *Pilar*

Este software permitió realizar un Análisis de Riesgos sobre las dimensiones de valoración disponibilidad, integridad y confidencialidad, aplicándose en 8 fases:

a) Datos del proyecto e identificación de activos

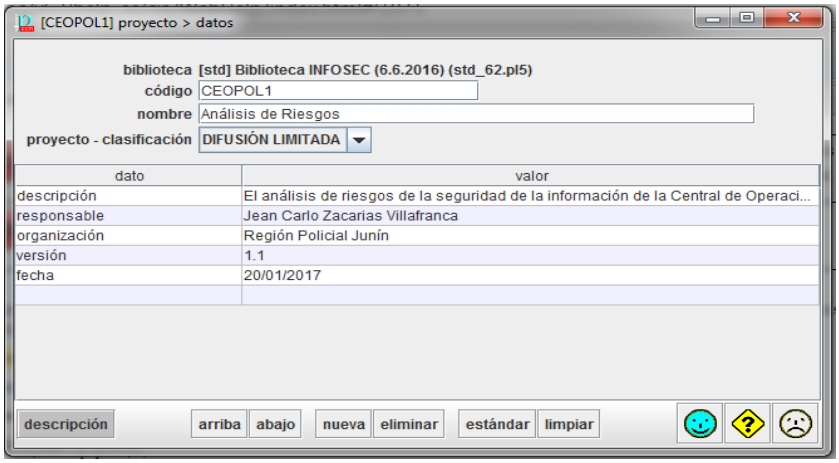


Figura 6. Datos del proyecto

Fuente: captura SW *PILAR*-Elaboración propia

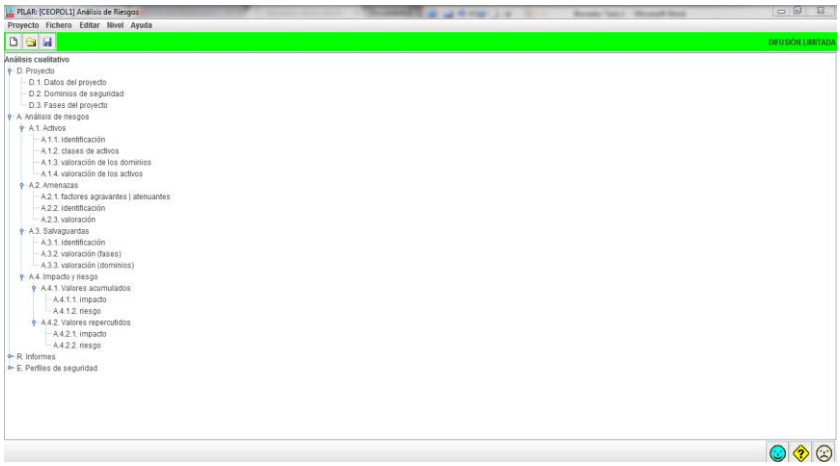


Figura 7. Identificación de los activos de información

Fuente: captura SW *PILAR*-Elaboración propia

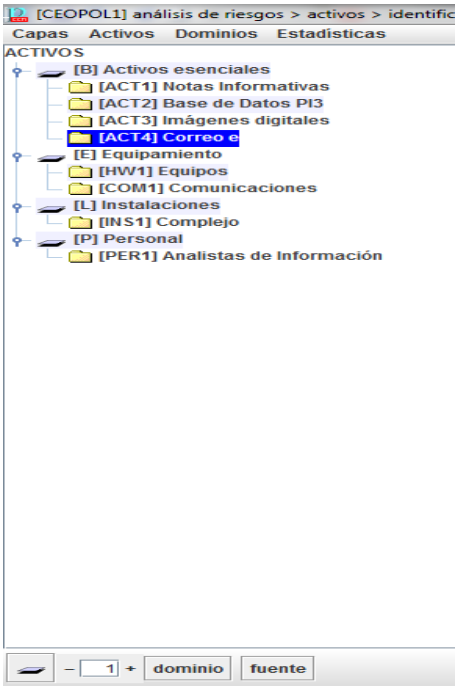


Figura 8. Nombramiento de los activos de información de la Ceopol

Fuente: captura SW *PILAR*-Elaboración propia

b) Identificación, dependencias y valoración de activos

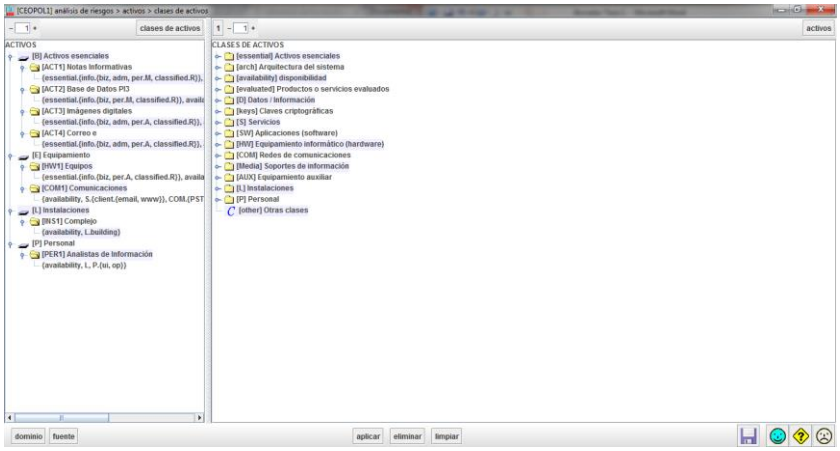


Figura 9. Identificación de los activos de información de la Ceopol

Fuente: captura SW *PILAR*-Elaboración propia

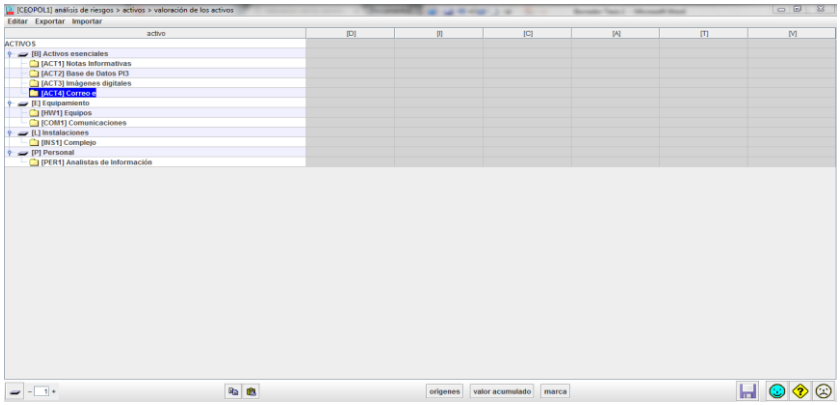


Figura 10. Dependencias de los activos de información de la Ceopol

Fuente: captura SW *Pilar*-Elaboración propia

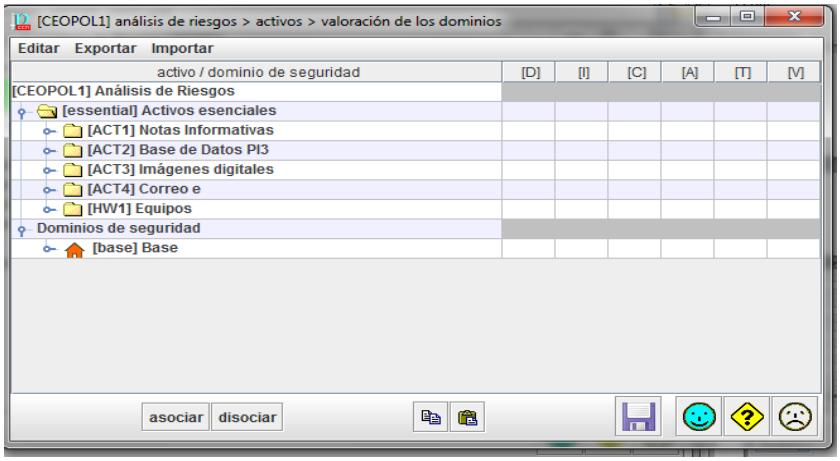


Figura 11. Valoración de los activos de información de la Ceopol

Fuente: captura SW *Pilar*-Elaboración propia

c) Determinación de amenazas, se identifican las posibles amenazas a las que están expuestas los activos identificados.

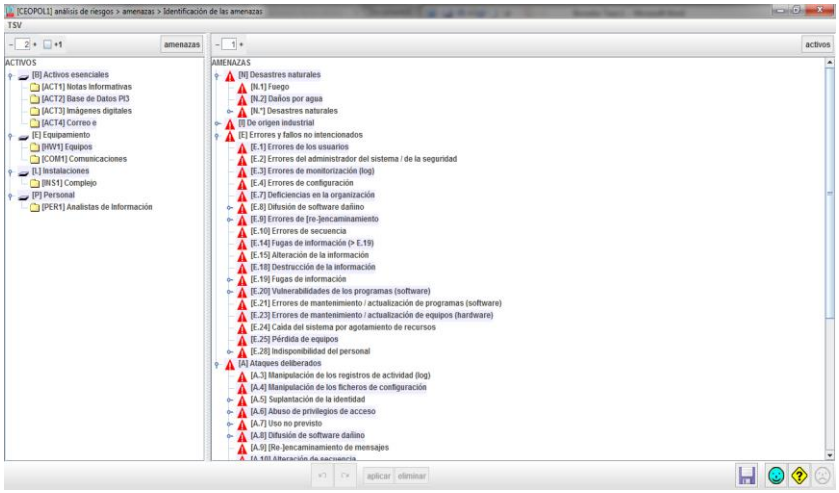


Figura 12. Determinación de amenazas - parte 1

Fuente: captura SW *Pilar*-Elaboración propia

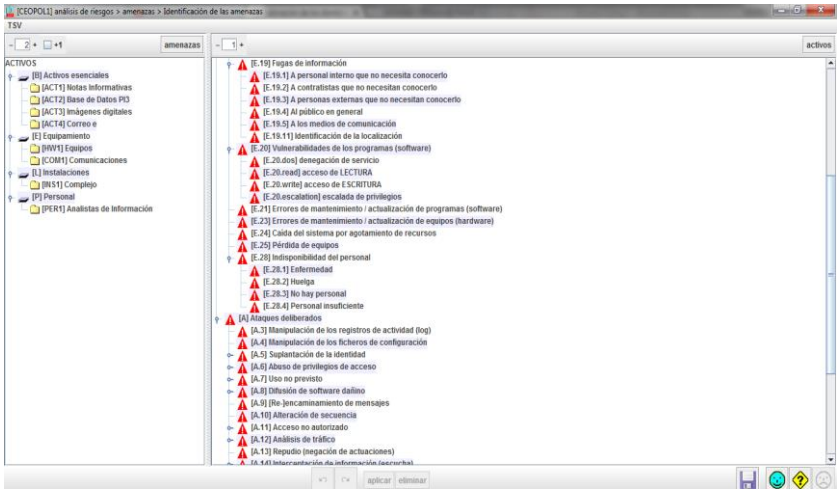


Figura 13. Determinación de amenazas - parte 2

Fuente: captura SW *Pilar*-Elaboración propia

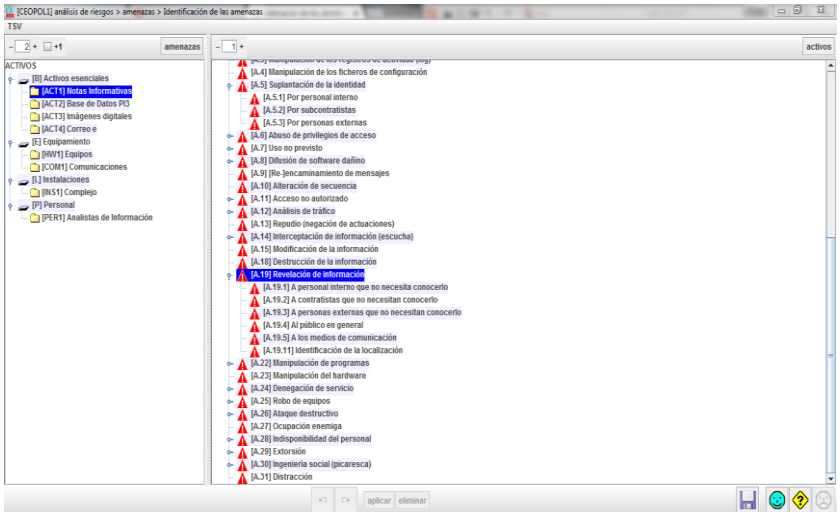


Figura 14. Determinación de amenazas - parte 3

Fuente: captura SW *Pilar*-Elaboración propia

d) Estimación de impactos, cuáles son las vulnerabilidades que pueden tener mayor impacto, en la escala de 1 a 10.

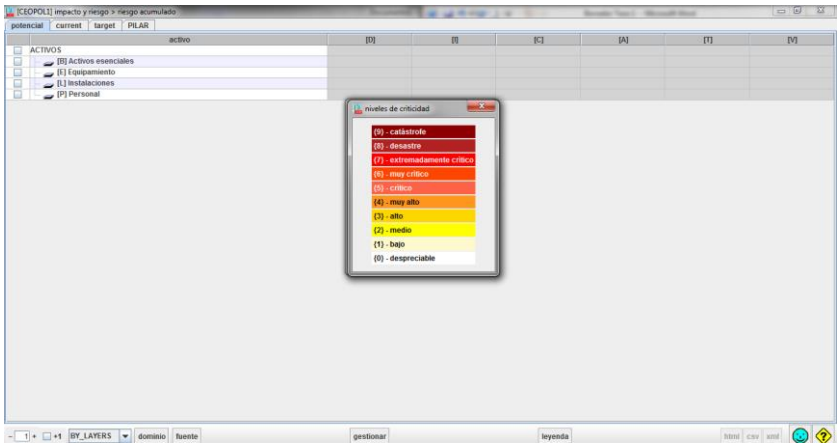


Figura 15. Estimación de impactos

Fuente: captura SW *Pilar*

Figura 16. Nivel de criticidad

Fuente: captura SW *Pilar*

e) Obtención de los riesgos de los activos de información identificados

Tabla 3. Resumen del nivel de impacto por activo de información y amenaza

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
Notas informativas	Fuego	1	3	3
	Daños por agua	1	3	3

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
Formato digital y físico	Desastres naturales	1	3	3
	Fuga de información	3	3	9
	Introducción de falsa información	3	3	9
	Alteración de la información	3	3	9
	Corrupción de la información	3	3	9
	Destrucción de información	3	3	9
	Corte del suministro eléctrico	1	1	1
	Condiciones inadecuadas de temperatura o humedad	1	1	1
	Fallo de servicios de comunicaciones	2	3	6
	Interrupción de otros servicios y suministros esenciales	2	1	2
	Degradación de los soportes de almacenamiento de la información	1	1	1
	Difusión de software dañino	1	3	3
	Errores de mantenimiento/ actualización de programas (software)	2	2	4
	Errores de mantenimiento/ actualización de equipos (hardware)	2	2	4
	Caída del sistema por sobrecarga	1	1	1
	Pérdida de equipos	1	3	3

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Indisponibilidad del personal	3	3	9
	Abuso de privilegios de acceso	3	3	9
	Acceso no autorizado	2	3	6
	Errores de los usuarios	3	3	9
	Errores del administrador	3	3	9
	Errores de configuración	1	3	3
	Denegación de servicio	1	1	1
	Indisponibilidad del personal	1	3	3
	Ingeniería social	2	3	6
Bases de datos PI3	Fuego	1	3	3
	Daños por agua	1	3	3
	Desastres naturales	1	3	3
	Fuga de información	3	3	9
	Introducción de falsa información	3	3	9
	Alteración de la información	3	3	9
	Corrupción de la información	3	3	9
	Destrucción de información	3	3	9
	Corte del suministro eléctrico	1	1	1
	Condiciones inadecuadas de temperatura o humedad	1	1	1
	Fallo de servicios de comunicaciones	2	3	6
	Interrupción de otros servicios y suministros esenciales	2	1	2

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Degradación de los soportes de almacenamiento de la información	1	1	1
	Difusión de software dañino	1	3	3
	Errores de mantenimiento/ actualización de programas (software)	2	2	4
	Errores de mantenimiento/ actualización de equipos (hardware)	2	2	4
	Caída del sistema por sobrecarga	1	1	1
	Pérdida de equipos	1	3	3
	Indisponibilidad del personal	3	3	9
	Abuso de privilegios de acceso	3	3	9
	Acceso no autorizado	2	3	6
	Errores de los usuarios	3	3	9
	Errores del administrador	3	3	9
	Errores de configuración	1	3	3
	Denegación de servicio	1	1	1
	Indisponibilidad del personal	1	3	3
	Ingeniería social	2	3	6
Imágenes digitales	Fuego	1	3	3
	Daños por agua	1	3	3
	Desastres naturales	1	3	3
	Fuga de información	3	3	9

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Introducción de falsa información	3	3	9
	Alteración de la información	3	3	9
	Corrupción de la información	3	3	9
	Destrucción de información	3	3	9
	Corte del suministro eléctrico	1	1	1
	Condiciones inadecuadas de temperatura o humedad	1	1	1
	Fallo de servicios de comunicaciones	2	3	6
	Interrupción de otros servicios y suministros esenciales	2	1	2
	Degradación de los soportes de almacenamiento de la información	1	1	1
	Difusión de software dañino	1	3	3
	Errores de mantenimiento/ actualización de programas (software)	2	2	4
	Errores de mantenimiento/ actualización de equipos (hardware)	2	2	4
	Caída del sistema por sobrecarga	1	1	1
	Pérdida de equipos	1	3	3
	Indisponibilidad del personal	3	3	9
	Abuso de privilegios de acceso	3	3	9

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Acceso no autorizado	2	3	6
	Errores de los usuarios	3	3	9
	Errores del administrador	3	3	9
	Errores de configuración	1	3	3
	Denegación de servicio	1	1	1
	Indisponibilidad del personal	1	3	3
	Ingeniería social	2	3	6
Correo electrónico comercial y *app Telegram Desktop*	Fuego	1	3	3
	Daños por agua	1	3	3
	Desastres naturales	1	3	3
	Fuga de información	3	3	9
	Introducción de falsa información	3	3	9
	Alteración de la información	3	3	9
	Corrupción de la información	3	3	9
	Destrucción de información	3	3	9
	Corte del suministro eléctrico	1	1	1
	Condiciones inadecuadas de temperatura o humedad	1	1	1
	Fallo de servicios de comunicaciones	2	3	6
	Interrupción de otros servicios y suministros esenciales	2	1	2
	Degradación de los soportes de almacenamiento de la información	1	1	1
	Difusión de software dañino	1	3	3

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Errores de mantenimiento/ actualización de programas (software)	2	2	4
	Errores de mantenimiento/ actualización de equipos (hardware)	2	2	4
	Caída del sistema por sobrecarga	1	1	1
	Pérdida de equipos	1	3	3
	Indisponibilidad del personal	3	3	9
	Abuso de privilegios de acceso	3	3	9
	Acceso no autorizado	2	3	6
	Errores de los usuarios	3	3	9
	Errores del administrador	3	3	9
	Errores de configuración	1	3	3
	Denegación de servicio	1	1	1
	Indisponibilidad del personal	1	3	3
	Ingeniería social	2	3	6
Ordenadores y equipos informáticos (HW)	Fuego	1	3	3
	Daños por agua	1	3	3
	Desastres naturales	1	3	3
	Fuga de información	3	3	9
	Introducción de falsa información	3	3	9
	Alteración de la información	3	3	9
	Corrupción de la información	3	3	9
	Destrucción de información	3	3	9

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Corte del suministro eléctrico	1	1	1
	Condiciones inadecuadas de temperatura o humedad	1	1	1
	Fallo de servicios de comunicaciones	2	3	6
	Interrupción de otros servicios y suministros esenciales	2	1	2
	Degradación de los soportes de almacenamiento de la información	1	1	1
	Difusión de software dañino	1	3	3
	Errores de mantenimiento/ actualización de programas (software)	2	2	4
	Errores de mantenimiento/ actualización de equipos (hardware)	2	2	4
	Caída del sistema por sobrecarga	1	1	1
	Pérdida de equipos	1	3	3
	Indisponibilidad del personal	3	3	9
	Abuso de privilegios de acceso	3	3	9
	Acceso no autorizado	2	3	6
	Errores de los usuarios	3	3	9
	Errores del administrador	3	3	9
	Errores de configuración	1	3	3
	Denegación de servicio	1	1	1

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Indisponibilidad del personal	1	3	3
	Ingeniería social	2	3	6
Conectividad, red LAN	Fuego	1	3	3
	Daños por agua	1	3	3
	Desastres naturales	1	3	3
	Fuga de información	3	3	9
	Introducción de falsa información	3	3	9
	Alteración de la información	3	3	9
	Corrupción de la información	3	3	9
	Destrucción de información	3	3	9
	Corte del suministro eléctrico	1	1	1
	Condiciones inadecuadas de temperatura o humedad	1	1	1
	Fallo de servicios de comunicaciones	2	3	6
	Interrupción de otros servicios y suministros esenciales	2	1	2
	Degradación de los soportes de almacenamiento de la información	1	1	1
	Difusión de software dañino	1	3	3
	Errores de mantenimiento/ actualización de programas (software)	2	2	4
	Errores de mantenimiento/ actualización de equipos (hardware)	2	2	4

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Caída del sistema por sobrecarga	1	1	1
	Pérdida de equipos	1	3	3
	Indisponibilidad del personal	3	3	9
	Abuso de privilegios de acceso	3	3	9
	Acceso no autorizado	2	3	6
	Errores de los usuarios	3	3	9
	Errores del administrador	3	3	9
	Errores de configuración	1	3	3
	Denegación de servicio	1	1	1
	Indisponibilidad del personal	1	3	3
	Ingeniería social	2	3	6
Instalaciones, infraestructura	Fuego	1	3	3
	Daños por agua	1	3	3
	Desastres naturales	1	3	3
	Fuga de información	3	3	9
	Introducción de falsa información	3	3	9
	Alteración de la información	3	3	9
	Corrupción de la información	3	3	9
	Destrucción de información	3	3	9
	Corte del suministro eléctrico	1	1	1
	Condiciones inadecuadas de temperatura o humedad	1	1	1
	Fallo de servicios de comunicaciones	2	3	6

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Interrupción de otros servicios y suministros esenciales	2	1	2
	Degradación de los soportes de almacenamiento de la información	1	1	1
	Difusión de software dañino	1	3	3
	Errores de mantenimiento/ actualización de programas (software)	2	2	4
	Errores de mantenimiento/ actualización de equipos (hardware)	2	2	4
	Caída del sistema por sobrecarga	1	1	1
	Pérdida de equipos	1	3	3
	Indisponibilidad del personal	3	3	9
	Abuso de privilegios de acceso	3	3	9
	Acceso no autorizado	2	3	6
	Errores de los usuarios	3	3	9
	Errores del administrador	3	3	9
	Errores de configuración	1	3	3
	Denegación de servicio	1	1	1
	Indisponibilidad del personal	1	3	3
	Ingeniería social	2	3	6
Personal, recursos	Fuego	1	3	3
	Daños por agua	1	3	3

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
Humanos, analistas de información	Desastres naturales	1	3	3
	Fuga de información	3	3	9
	Introducción de falsa información	3	3	9
	Alteración de la información	3	3	9
	Corrupción de la información	3	3	9
	Destrucción de información	3	3	9
	Corte del suministro eléctrico	1	1	1
	Condiciones inadecuadas de temperatura o humedad	1	1	1
	Fallo de servicios de comunicaciones	2	3	6
	Interrupción de otros servicios y suministros esenciales	2	1	2
	Degradación de los soportes de almacenamiento de la información	1	1	1
	Difusión de software dañino	1	3	3
	Errores de mantenimiento/ actualización de programas (software)	2	2	4
	Errores de mantenimiento/ actualización de equipos (hardware)	2	2	4
	Caída del sistema por sobrecarga	1	1	1
	Pérdida de equipos	1	3	3
	Indisponibilidad del personal	3	3	9

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
	Abuso de privilegios de acceso	3	3	9
	Acceso no autorizado	2	3	6
	Errores de los usuarios	3	3	9
	Errores del administrador	3	3	9
	Errores de configuración	1	3	3
	Denegación de servicio	1	1	1
	Indisponibilidad del personal	1	3	3
	Ingeniería social	2	3	6

Fuente: Elaboración propia

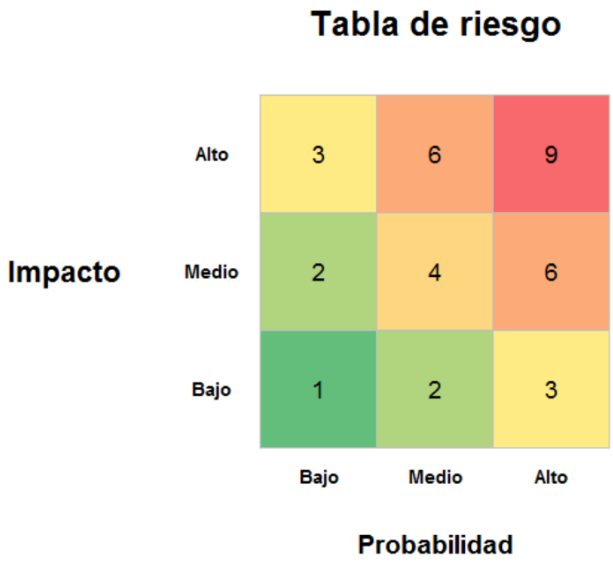


Figura 17. Indicador de riesgo según valoración

Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

f) Interpretación de los riesgos de los activos de información identificados

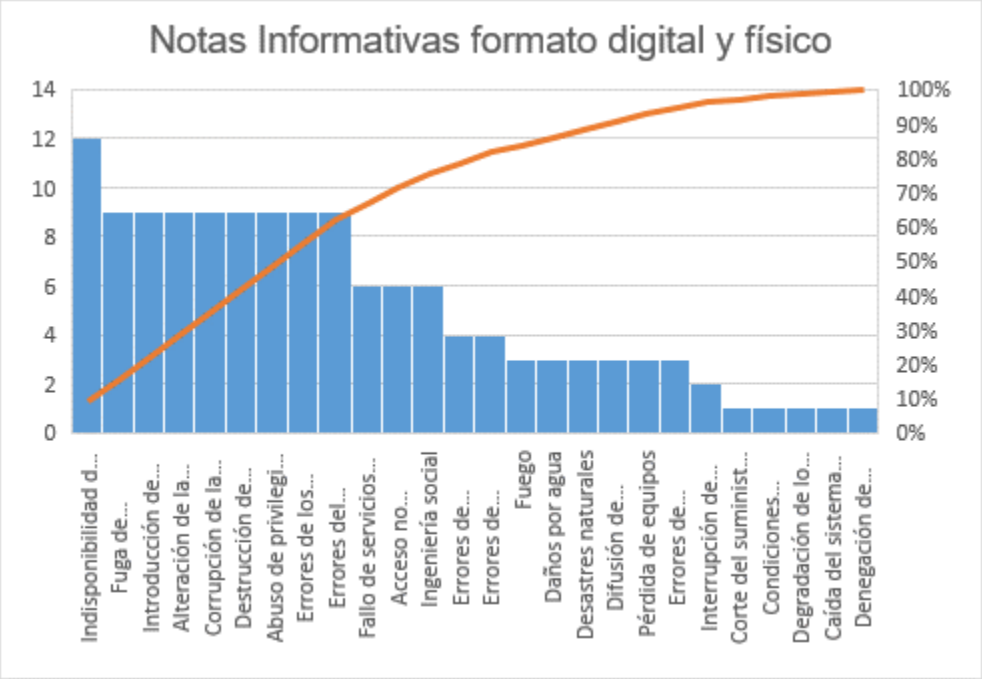


Figura 18. Activo de información: notas informativas

Fuente: Elaboración propia

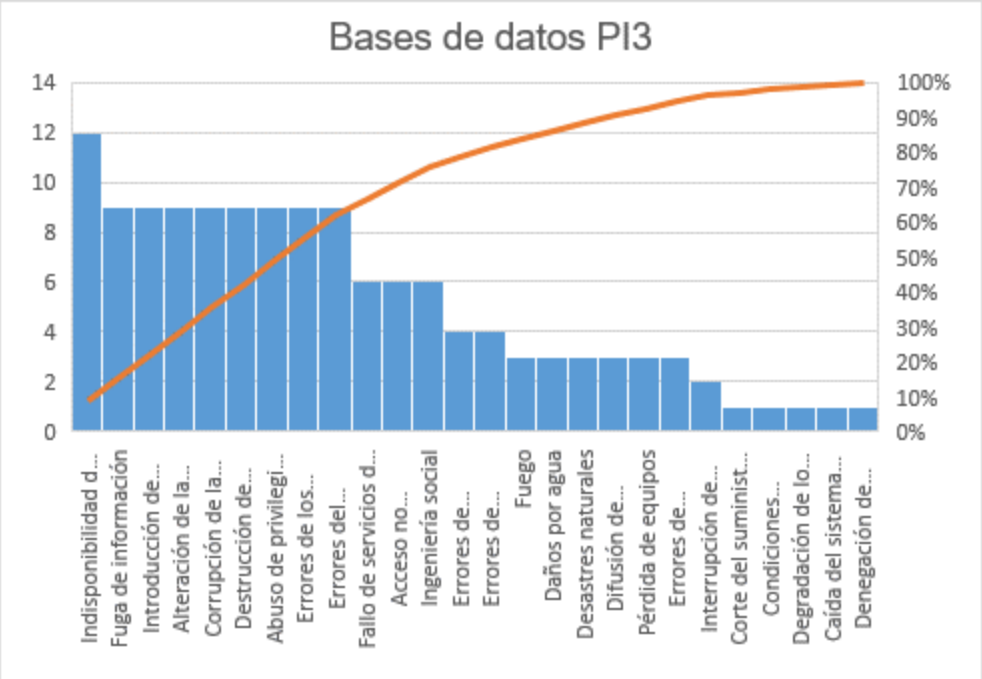


Figura 19. Activo de información: bases de datos PI3

Fuente: Elaboración propia

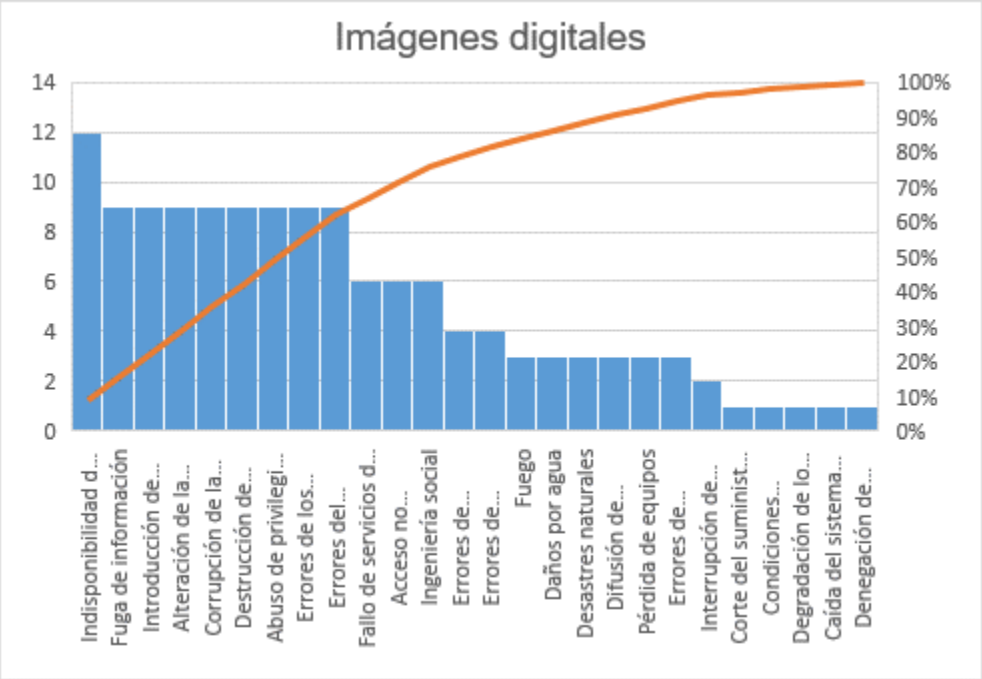


Figura 20. Activo de información: imágenes digitales

Fuente: elaboración propia

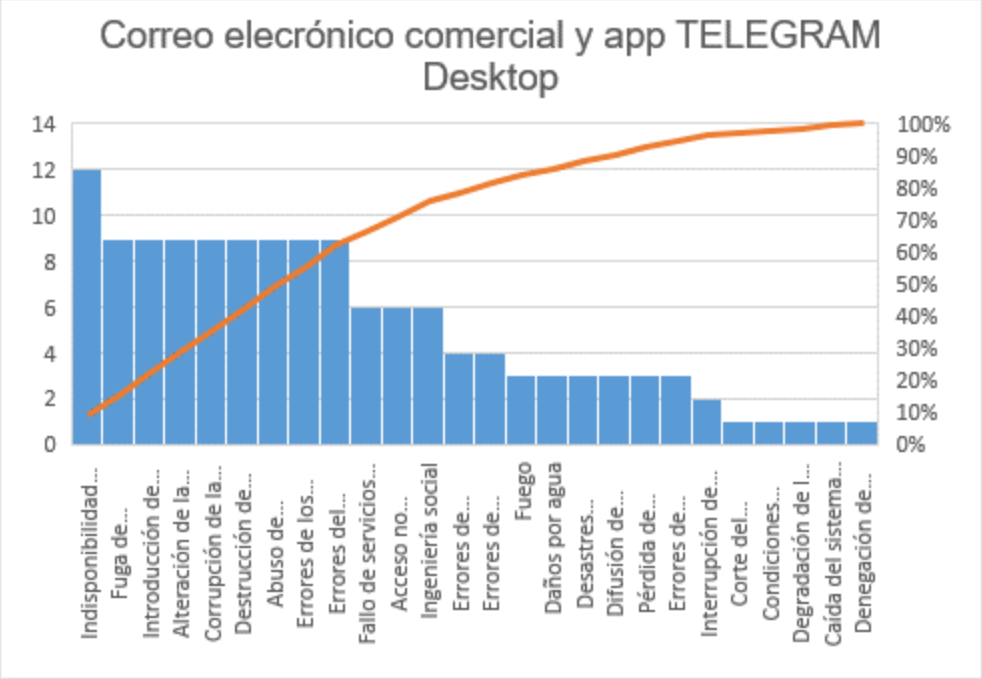


Figura 21. Activo de información: correo electrónico comercial y app Telegram

Fuente: elaboración propia

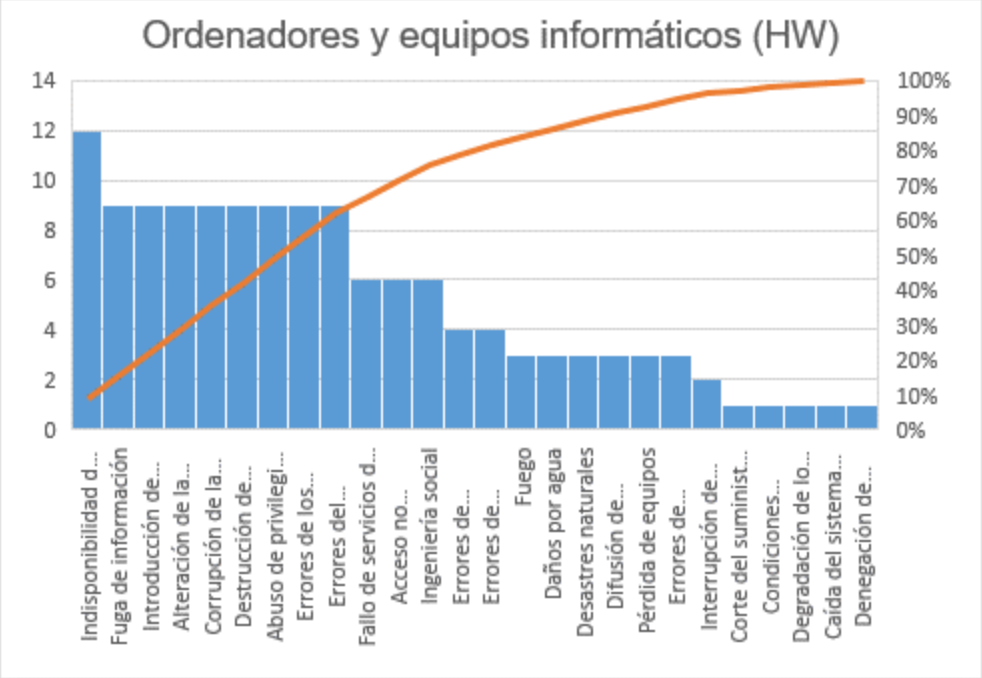


Figura 22. Activo de información: ordenadores y equipos informáticos (HW)

Fuente: elaboración propia

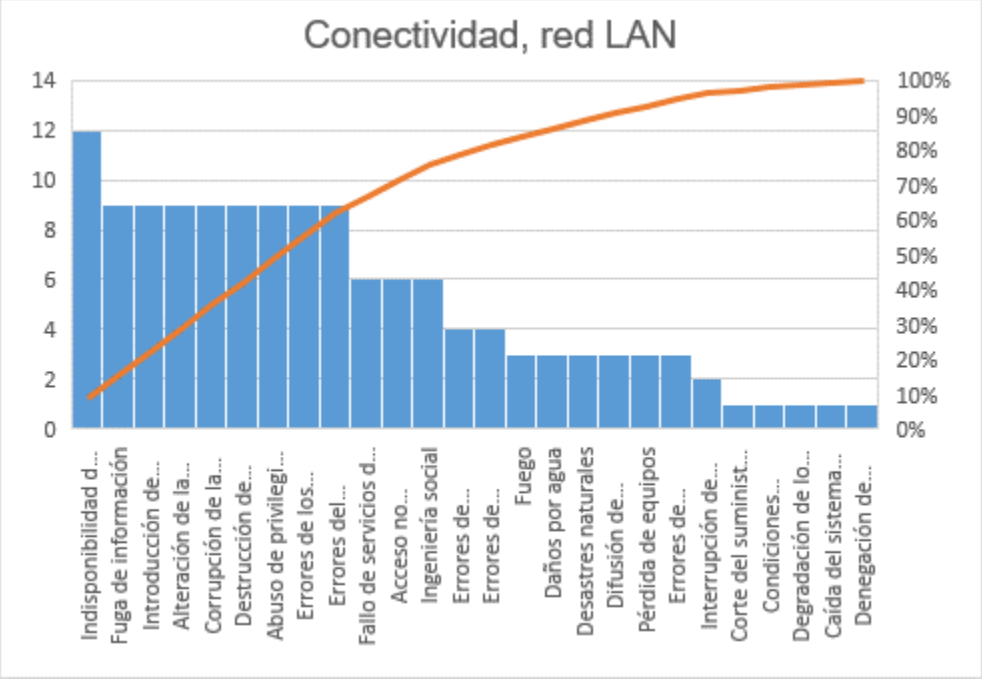


Figura 23. Activo de información: conectividad, red LAN

Fuente: elaboración propia

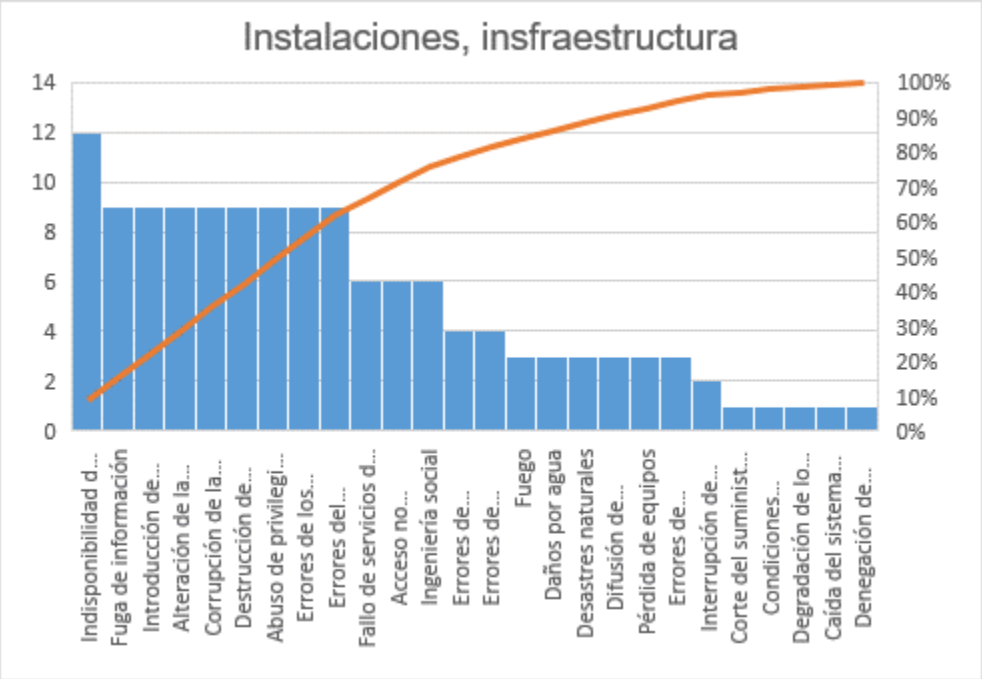


Figura 24. Activo de información: instalación e infraestructura

Fuente: elaboración propia

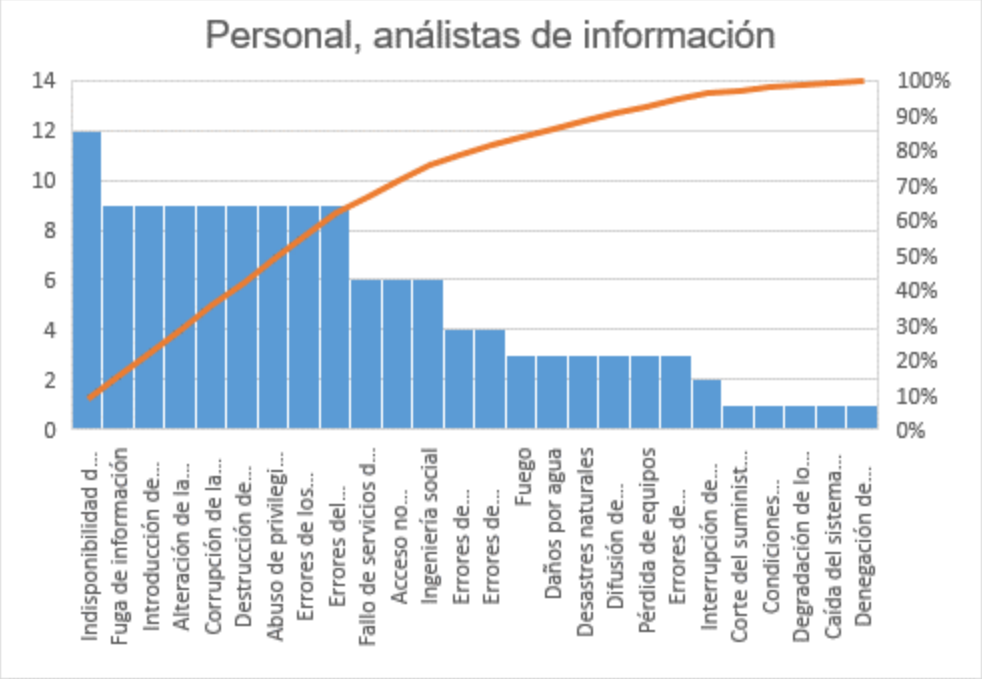


Figura 25. Activo de información: personal policial, analistas de información

Fuente: elaboración propia

g) Determinación de los criterios de aceptación del riesgo, determinamos cómo se encuentra el riesgo acumulado.

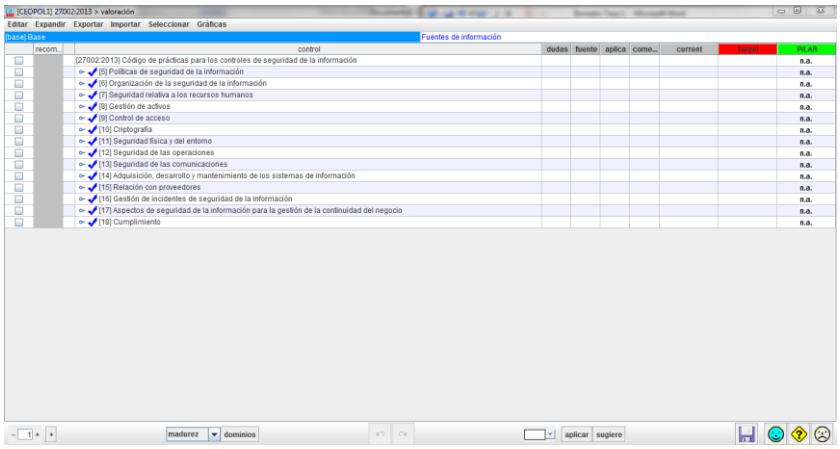


Figura 26. Identificación del riesgo acumulado parte 1

Fuente: captura SW *Pilar*-Elaboración propia

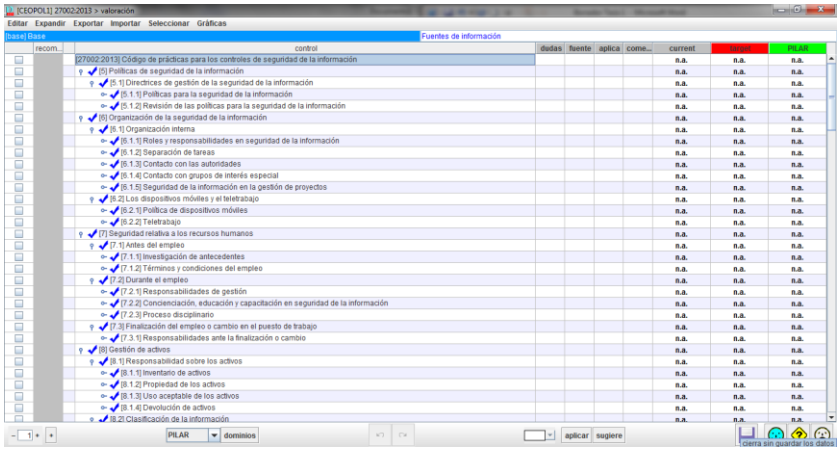


Figura 27. Identificación del riesgo acumulado parte 2

Fuente: captura SW *Pilar*-Elaboración propia

Figura 28. Identificación del riesgo acumulado parte 3

Fuente: captura SW *Pilar*-Elaboración propia

Figura 29. Identificación del riesgo acumulado parte 4

Fuente: captura SW *Pilar*-Elaboración propia

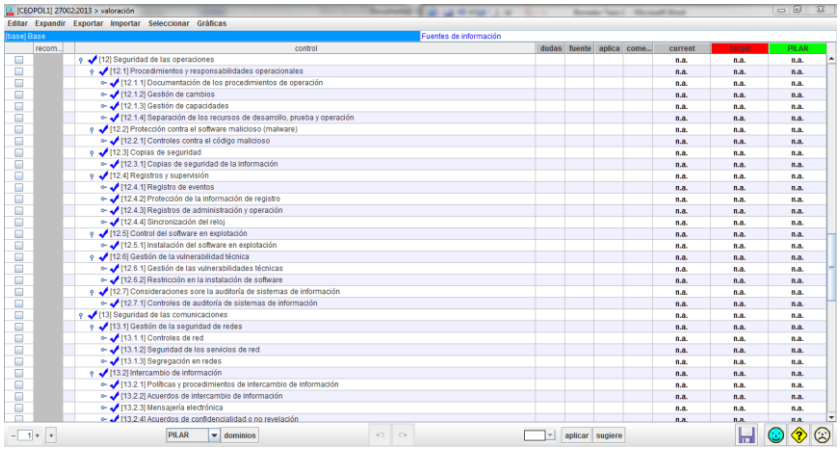


Figura 30. Identificación del riesgo acumulado parte 5

Fuente: captura SW *Pilar*-Elaboración propia

Figura 31. Identificación del riesgo acumulado parte 6

Fuente: captura SW *Pilar*-Elaboración propia

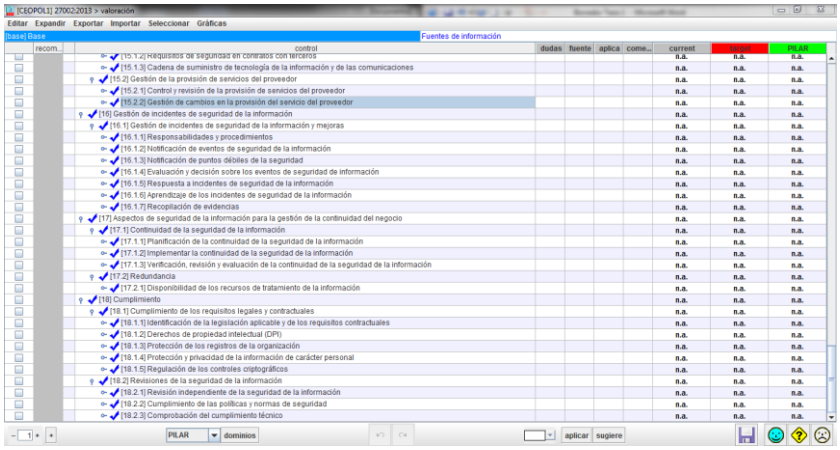


Figura 32. Identificación del riesgo acumulado parte 7

Fuente: captura SW *Pilar*-Elaboración propia

h) Determinación de las medidas de seguridad necesarias o salvaguardas, recursos para mitigar el impacto del riesgo.

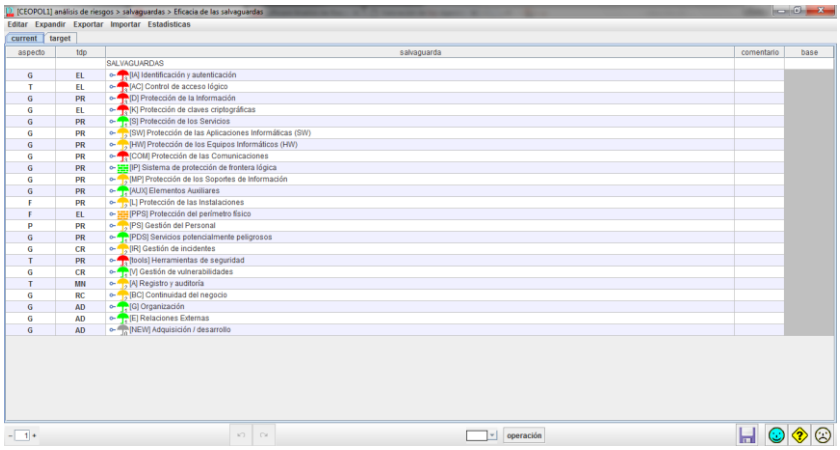


Figura 33. Determinación de Salvaguardas

Fuente: captura SW *Pilar*-Elaboración propia

4.2.2 Conclusiones del análisis de riesgos

- La metodología *Magerit* por medio de la herramienta *Pilar*, facilitó realizar un análisis de riesgos de la seguridad de la información de la Central de Operaciones Policiales de la Región Policial Junín, para garantizar la seguridad de los activos de información, identificando como las amenazas y vulnerabilidades más frecuentes a los siguientes factores:
  - Indisponibilidad del personal
  - Fuga de información
  - Introducción de falsa información

- Alteración de la información
- Corrupción de la información y
- Destrucción de información.

- El análisis de riesgo aplicado, permite conocer de manera global el estado actual de la seguridad de la información en la Central de Operaciones Policiales de la Región Policial Junín.
- La evaluación informática permite mejorar la madurez en los dominios y la formulación de un documento que norme las políticas de seguridad de la información.
- La metodología *Magerit* y su herramienta *Pilar*, se adapta a cualquier tipo de organización para la ejecución del análisis de riesgos de los activos de información.

CAPÍTULO V
RESULTADOS Y DISCUSIÓN

5.1 Tratamiento y análisis de la información

5.1.1 Análisis de fiabilidad del instrumento

Para iniciar el trabajo de investigación se elaboró un cuestionario como instrumento de recolección de datos, seguidamente se validó la fiabilidad de los datos recolectados mediante el Alfa de Cronbach como se muestra en la Tabla 4.

Tabla 4. Resumen de procesamiento de casos

		N	%
Casos	**Válido**	32	100,0
	Excluido[a]	0	,0
	Total	32	100,0
a. La eliminación por lista se basa en todas las variables del procedimiento.			

Fuente: elaboración propia

Tabla 5. Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,762	49

Fuente: elaboración propia

En la tabla 5 responde a un Alfa de Cronbach total de 0,762 el cual demuestra que el instrumento es fiable de acuerdo al criterio general de George y Mallery.

5.1.2 Análisis descriptivo de las dimensiones

En el presente trabajo de investigación se aplicaron Políticas de Seguridad previo análisis de riesgos basados en la metodología *MAGERIT* para evaluar la influencia de un modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín; en ese sentido, se aplicó un pretest que nos permitió conocer el estado inicial de la dimensiones; seguidamente, se implementó el Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2013, para pasar a evaluar nuevamente con un postest. A continuación, se muestran los resultados descriptivos de estas medidas en las tablas 6, 9 y 12.

a. Dimensión amenazas

En la tabla 6 se observan los resultados descriptivos de la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

En las tablas 7 y 8 se observan las medidas descriptivas del Pretest y Postest de la dimensión amenazas, donde se observa pretest y postest, la influencia significativa de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Tabla 6. Estadísticos de la dimensión amenazas

		Pretest Amenazas	Postest Amenazas
N	**Válido**	32	32
	Perdidos	0	0
Media		1,30	4,94
Error estándar de la media		,037	,020
Mediana		1,24	5,00
Moda		1	5
Desviación estándar		,210	,112
Varianza		,044	,012
Rango		1	1
Mínimo		1	5
Máximo		2	5
Suma		41	158
Percentiles	25	1,15	4,91
	50	1,24	5,00
	75	1,37	5,00

Fuente: elaboración propia

Tabla 7. Frecuencias pretest Amenazas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Probablemente NO	32	100,0	100,0	100,0
	Total	32	0.0	0	

Fuente: elaboración propia

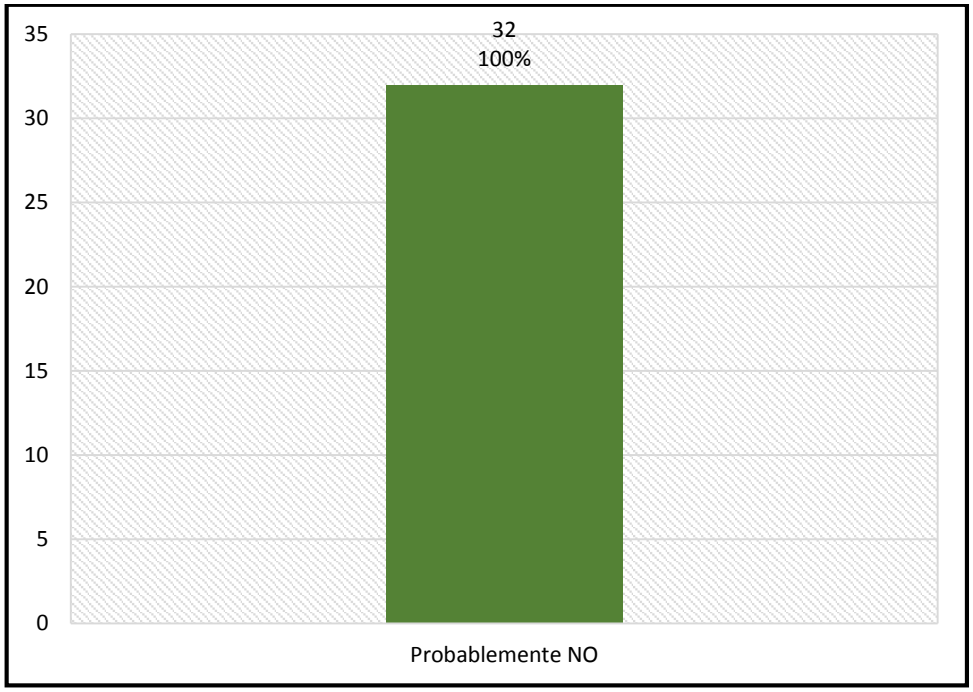


Figura 34. Frecuencia pretest - Dimensión Amenazas

Fuente: elaboración propia

Tabla 8. Frecuencias postest Amenazas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Definitivamente SÍ	32	0.0	100	100,0
	Total	32	0.0	100	

Fuente: elaboración propia

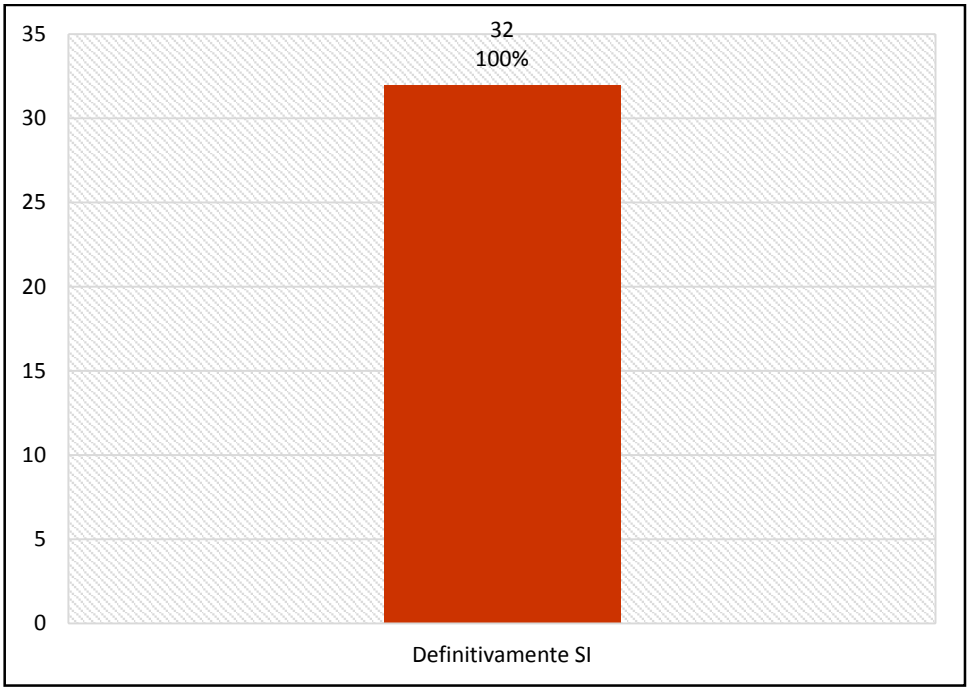


Figura A. Frecuencia postest - Dimensión Amenazas

Fuente: elaboración propia

En el caso de la dimensión amenaza, el pretest de la muestra resultó un valor de 1,30 que representa el 26%, mientras que, en el postest fue de 4,94 que representa el 99%, esto revela una diferencia considerable pre y postimplementación del modelo de seguridad de la información basado en la Norma ISO/IEC 27001:2013; asimismo, el nivel de diferencia mínimo pre fue de 1 que representa el 20% y post fue de 5 que representa el 100% como se puede apreciar en la figura 36.

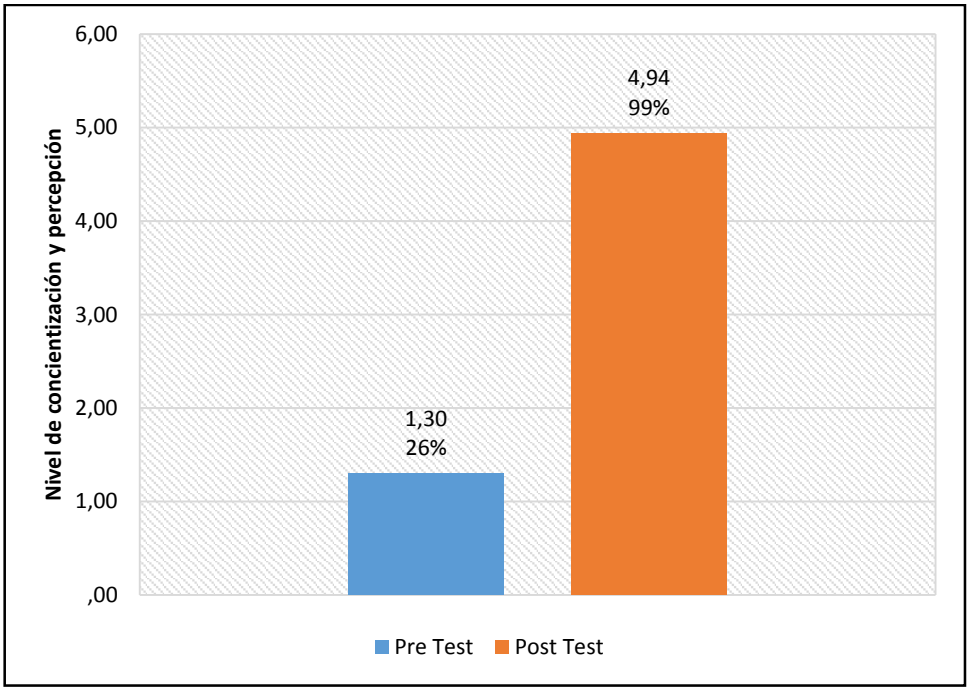


Figura 36. Dimensión amenazas pre y postest de implementado el SGSI

Fuente: elaboración propia

b. Dimensión vulnerabilidades

En la tabla 9 se observan los resultados descriptivos de la influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

En las tablas 10 y 11 se observan las medidas descriptivas del pretest y postest de la dimensión vulnerabilidades, donde se observa en el pretest y postest la influencia significativa de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Tabla 9. Estadísticos de la dimensión vulnerabilidades

		Pretest Vulnerabilidades	Postest Vulnerabilidades
N	**Válido**	32	32
	Perdidos	0	0
Media		1,50	5,00
Error estándar de la media		,090	,000
Mediana		1,50	5,00
Moda		1[a]	5
Desviación estándar		,508	,000
Varianza		,258	,000
Rango		1	0
Mínimo		1	5
Máximo		2	5
Suma		48	160
Percentiles	25	1,00	5,00
	50	1,50	5,00
	75	2,00	5,00

Fuente: elaboración propia

Tabla 10. Frecuencias pretest Vulnerabilidades

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Definitivamente NO	16	50.0	50	50.0
	Probablemente NO	16	50.0	50	100.0
	Total	32	100.0	100	

Fuente: elaboración propia

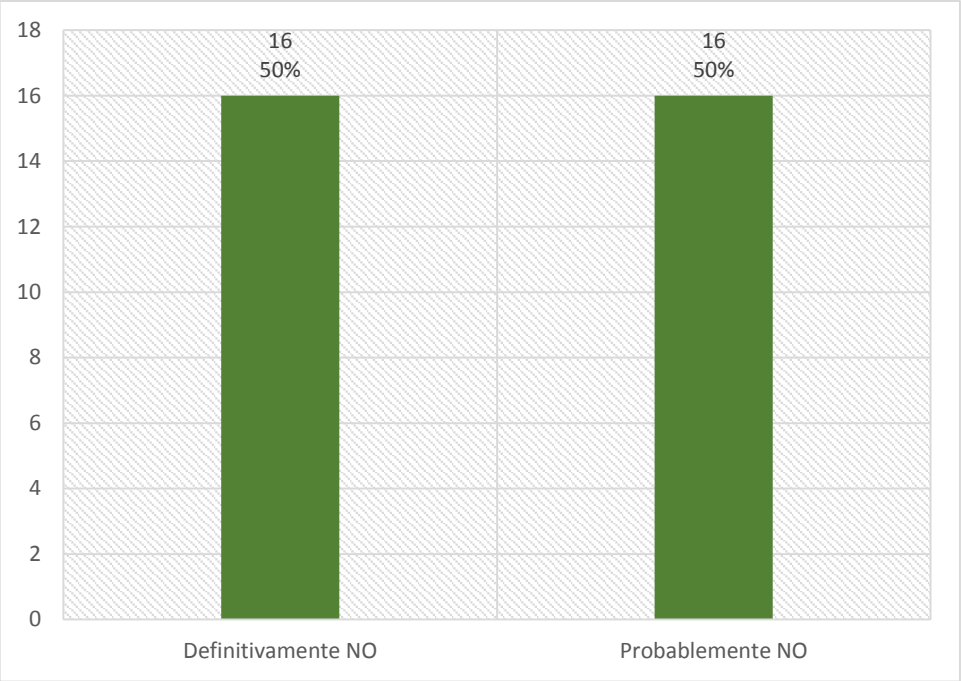


Figura 37. Frecuencia pretest - Dimensión Vulnerabilidades

Fuente: elaboración propia

Tabla 11. Frecuencias postest Vulnerabilidades

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Definitivamente SÍ	32	100.0	100	100,0
	Total	32	100.0	100	

Fuente: elaboración propia

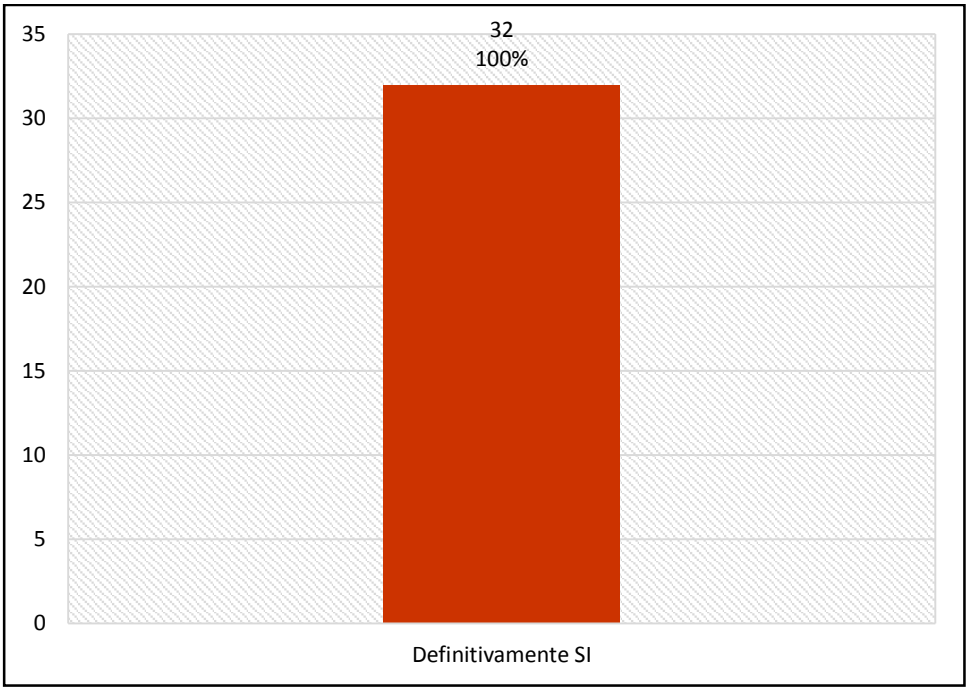


Figura 38. Frecuencia postest - Dimensión Vulnerabilidades

Fuente: elaboración propia

En el caso de la dimensión vulnerabilidades, el pretest de la muestra resultó un valor de 1,50 que representa el 30%, mientras que en el postest fue de 5,00 que representa el 100%, esto revela una diferencia considerable pre y postimplementación del modelo de seguridad de la información basado en la Norma ISO/IEC 27001:2013; asimismo, el nivel de diferencia mínimo pre fue de 1 que representa el 20% y post fue de 5 que representa el 100% como se puede apreciar en la figura 39.

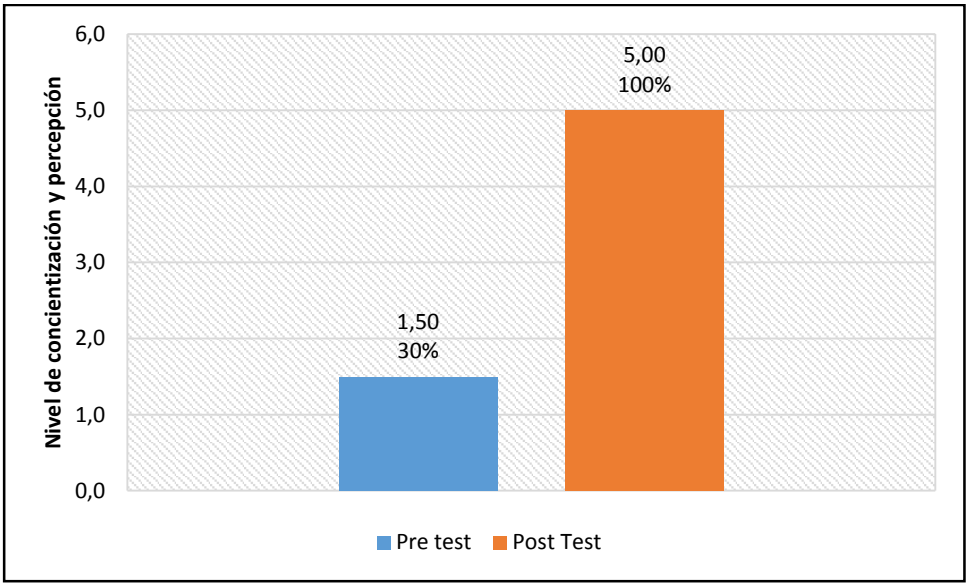


Figura 39. Dimensión vulnerabilidades pre y postest de implementado el SGSI

Fuente: elaboración propia

c. Dimensión sistema de gestión de seguridad de la información

En la tabla 12 se observan los resultados descriptivos de la influencia de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

En las tablas 13 y 14 se observan las medidas descriptivas del pretest y postest de la dimensión sistema de gestión de seguridad de la información, donde se observa en el pretest y postest la influencia significativa de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Tabla 12. Estadísticos de la dimensión sistema de gestión de seguridad de la información

		Pretest modelo de seguridad	Postest modelo de seguridad
N	Válido	32	32
	Perdidos	0	0
Media		1.22	4.96
Error estándar de la media		.030	.015
Mediana		1.14	5.00
Moda		1[a]	5
Desviación estándar		.172	.085
Varianza		.030	.007
Asimetría		.818	-3.220
Error estándar de asimetría		.414	.414
Curtosis		-.779	11.407
Error estándar de curtosis		.809	.809
Rango		1	
Mínimo		1	5
Máximo		2	5
Suma		39	159
Percentiles	25	1.10	4.95
	50	1.14	5.00
	75	1.40	5.00

Fuente: elaboración propia

Tabla 13. Frecuencias pretest sistema de gestión de seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Definitivamente NO	29	90.6	90.6	90.6
	Probablemente NO	3	9.4	9.4	100.0
	Total	32	100.0	100.0	

Fuente: elaboración propia

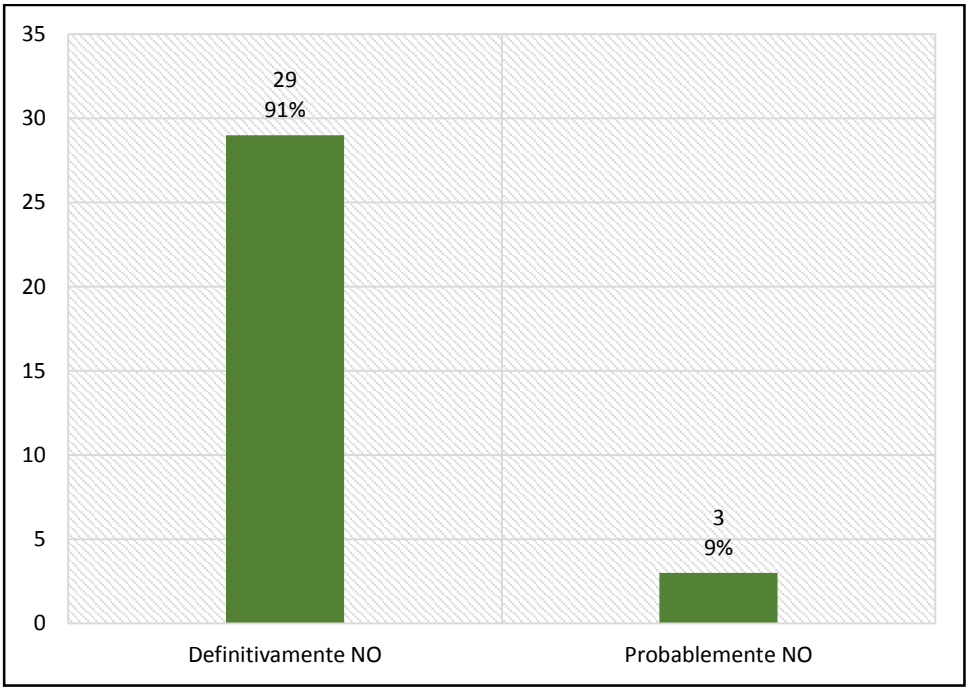


Figura 40. Frecuencia pretest - Dimensión sistema de gestión de seguridad de la información

Fuente: elaboración propia

Tabla 14. Frecuencias postest sistema de gestión de seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Definitivamente SÍ	32	100.0	100	100,0
	Total	32	100.0	100	

Fuente: elaboración propia

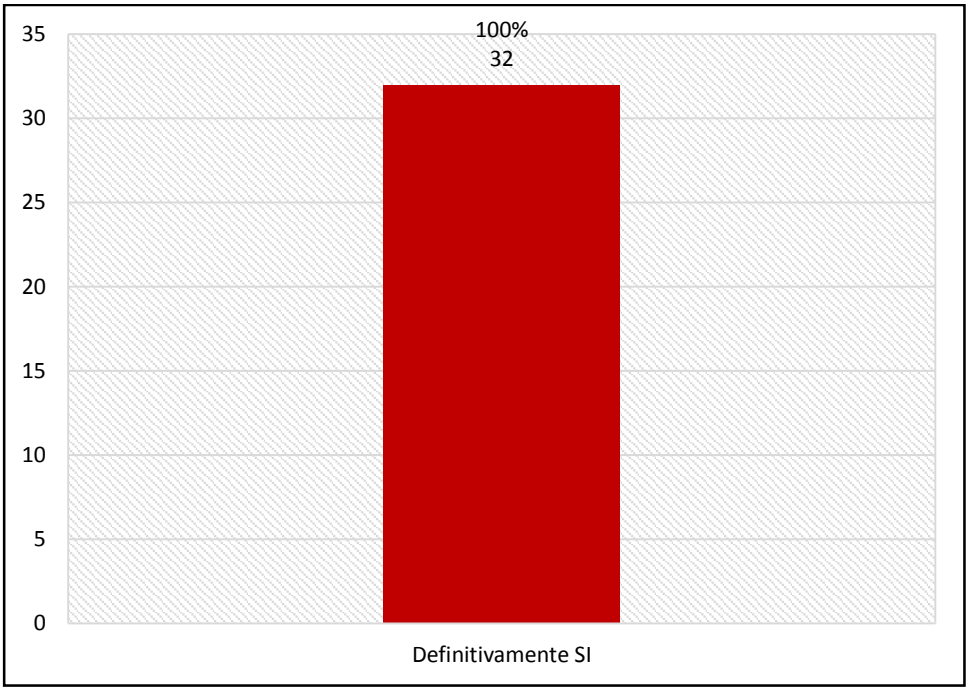


Figura 41. Frecuencia postest - Dimensión sistema de gestión de seguridad de la información

Fuente: elaboración propia

En el caso de la dimensión sistema de gestión de seguridad de la información, el pretest de la muestra resultó un valor de 1,22 que representa el 24%, mientras que en el postest fue de 4,96 que representa el 99%, esto revela una diferencia considerable pre y postimplementación del modelo de seguridad de la información basado en la Norma ISO/IEC 27001:2013; asimismo, el nivel de diferencia mínimo pre fue de 1 que representa el 20% y post fue de 5 que representa el 100% como se puede apreciar en la figura 42.

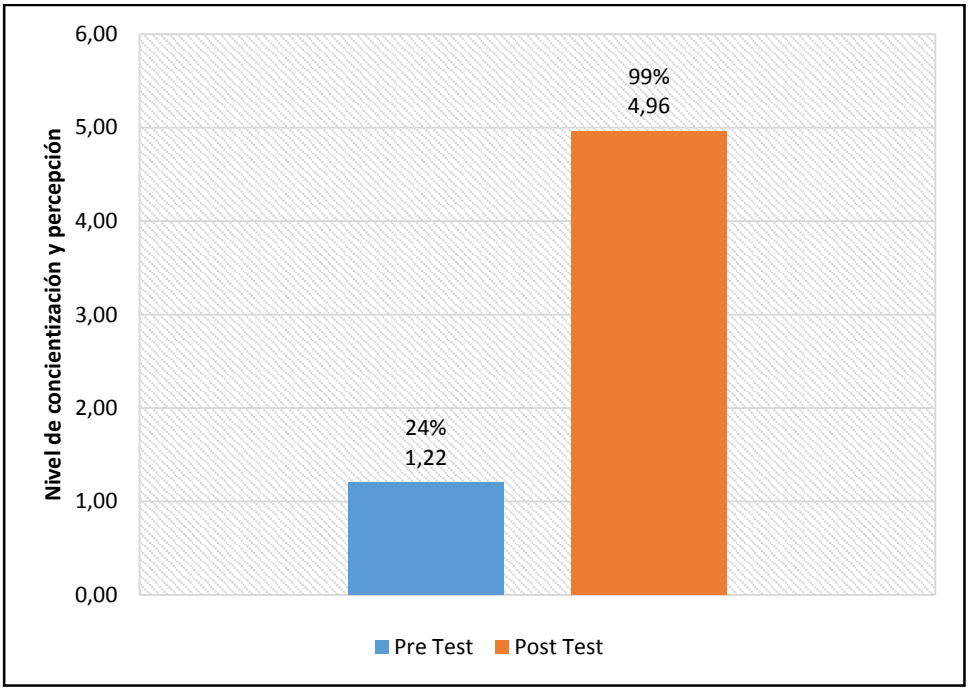


Figura 42. Dimensión sistema de gestión de seguridad de la información pre y postest de implementado el SGSI

Fuente: elaboración propia

5.1.3 Análisis inferencial

Pruebas de normalidad

Procedemos a realizar la prueba de normalidad a las dimensiones amenazas y vulnerabilidades para evaluar la influencia de un modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, a través de la Prueba de Shapiro-Wilk, ya que el tamaño de la muestra es menor a 50. La prueba estadística fue desarrollada en el software SPSS versión 23.0, el nivel de confiabilidad fue del 95%, bajo las siguientes condiciones:

Si:

Sig. < 0.05 = adopta una distribución no normal

Sig. > 0.05 = adopta una distribución normal

Donde:

Sig.: p - valor o nivel crítico del contraste

A continuación, se muestran los resultados:

a. Dimensión amenazas

Con el fin de seleccionar la prueba de hipótesis, los datos fueron sometidos a la comprobación de su distribución.

En la tabla 15 se observa como resultado la prueba de normalidad para el pretest de la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Tabla 15. Pruebas de normalidad pretest Amenazas

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pretest Amenazas	.875	32	.002

Fuente: elaboración propia

Como se observa en la tabla 15 el valor de Sig. del pretest de la dimensión amenazas en la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, es menor a 0.05, por ello se determina una distribución no normal.

En la tabla 16 se observa como resultado la prueba de normalidad del postest de la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Tabla 16. Pruebas de normalidad postest Amenazas

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pretest Amenazas	.875	32	.002
	Shapiro-Wilk		
	Estadístico	gl	Sig.
Postest Amenazas	.623	32	.000

Fuente: elaboración propia

Como se observa en la tabla 16 el valor de Sig. del postest de la dimensión amenazas en la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, es menor a 0.05, por ello se determina una distribución no normal.

Estadístico descriptivo

En la figura 43, se muestra el pretest de la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, obteniendo una media de 1,30 y una desviación estándar de 0,210.

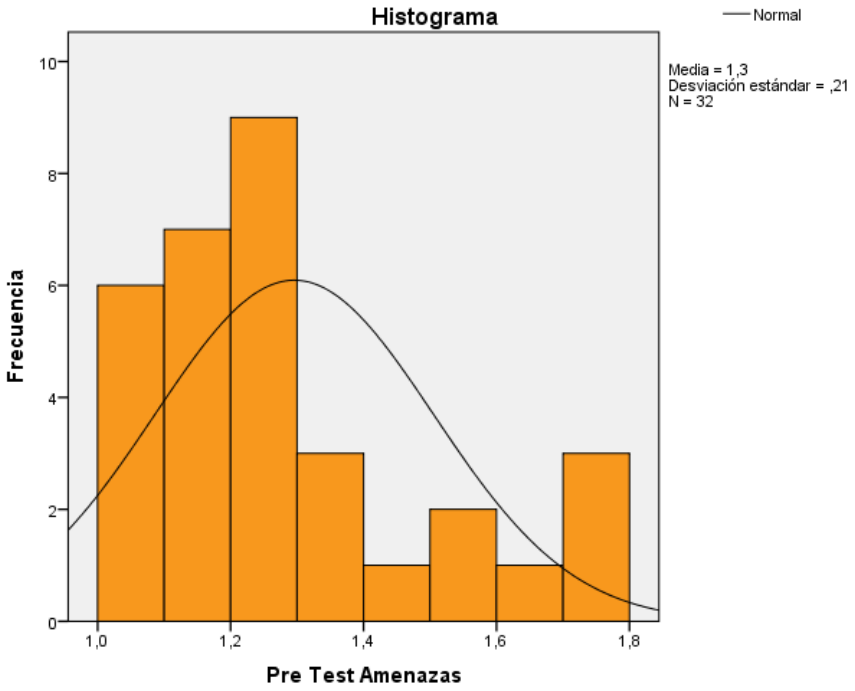


Figura 43. Pretest de la Influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín

Fuente: elaboración propia

En la figura 44, se muestra el postest de la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, obteniendo una media de 4,94 y una desviación estándar de 0,112.

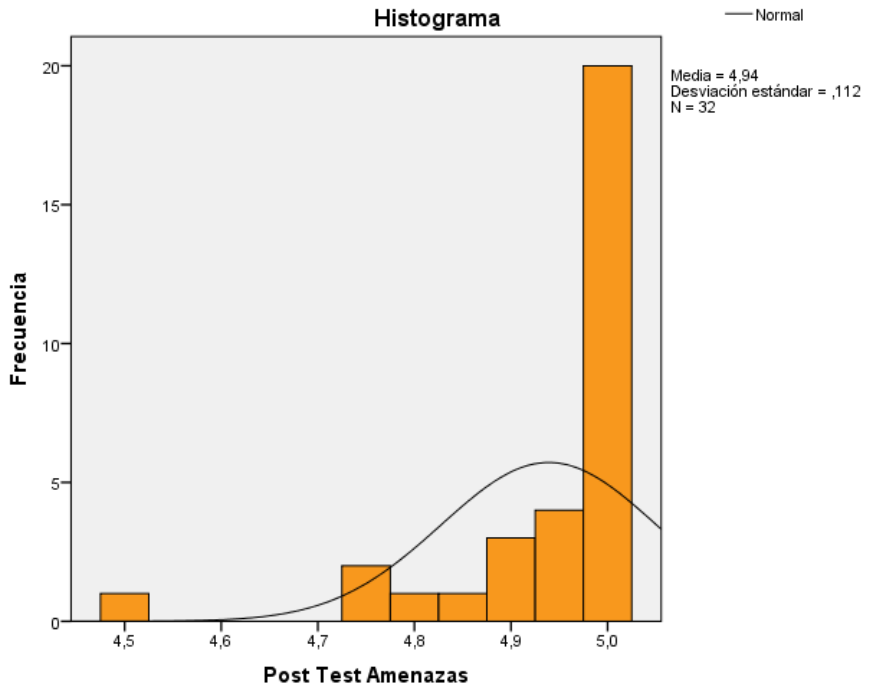


Figura 44. Postest de la Influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín

Fuente: elaboración propia

Tomando los resultados de las figuras anteriores, se observa que existe un aumento considerable en la mitigación de la dimensión amenazas dada la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, desde 1,30 hasta 4,94.

b. Dimensión vulnerabilidades

Con el fin de seleccionar la prueba de hipótesis, los datos fueron sometidos a la comprobación de su distribución.

En la tabla 17 se observa como resultado la prueba de normalidad para el pretest de la influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Tabla 17. Pruebas de normalidad pretest Vulnerabilidades

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pretest Vulnerabilidades	.741	32	.000

Fuente: elaboración propia

Como se observa en la tabla 17 el valor de Sig. del pretest de la dimensión vulnerabilidades en la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, es menor a 0,05, por ello se determina una distribución no normal.

En la tabla 18 se observa como resultado la prueba de normalidad del postest de la influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Tabla 18. Pruebas de normalidad postest Vulnerabilidades

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Postest Vulnerabilidades	.172	32	.000

Fuente: elaboración propia

Como se observa en la tabla 18 el valor de Sig. del Postest de la dimensión vulnerabilidades en la influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, es menor a 0,05, por ello se determina una distribución no normal.

Estadístico descriptivo

En la figura 45, se muestra el pretest de la influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, obteniendo una media de 1,15 y una desviación estándar de 0,202.

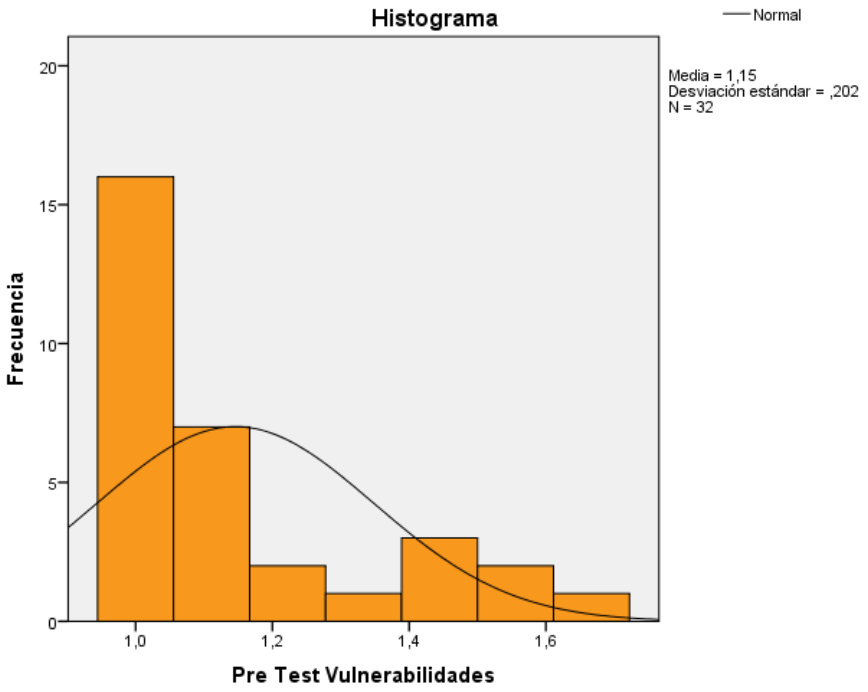


Figura 45. Pretest de la Influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín

Fuente: elaboración propia

En la figura 46, se muestra el postest de la influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, obteniendo una media de 4,98 y una desviación estándar de 0,098.

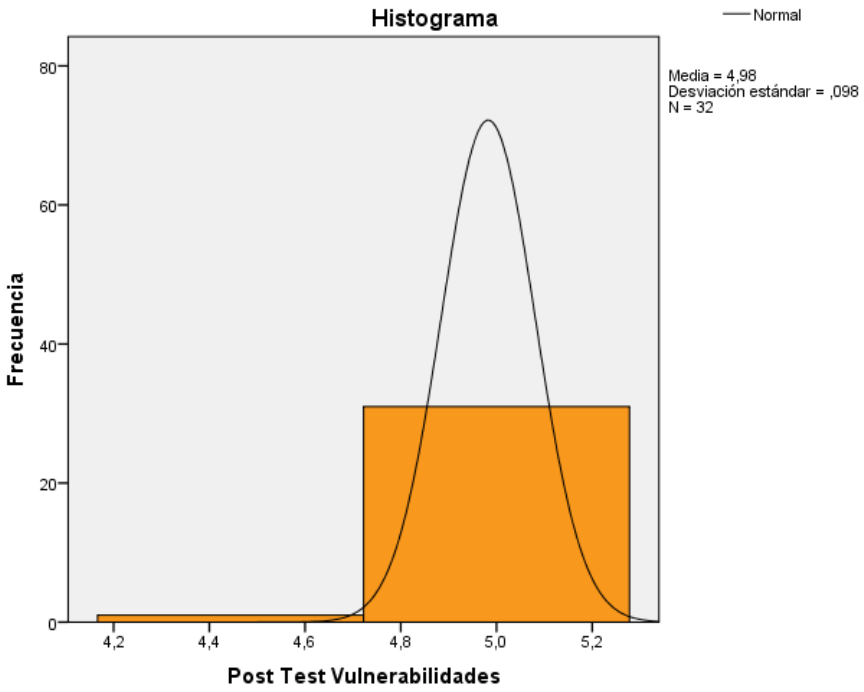


Figura 46. Postest de la Influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín

Fuente: elaboración propia

Tomando los resultados de las figuras anteriores, se observa que existe un aumento considerable en la mitigación de la dimensión vulnerabilidades dada la influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, desde 1,15 hasta 4,98.

c. Dimensión sistema de gestión de seguridad de la información

Con el fin de seleccionar la prueba de hipótesis, los datos fueron sometidos a la comprobación de su distribución.

En la tabla 19 se observa como resultado la prueba de normalidad para el pretest de la influencia de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Tabla 19. Pruebas de normalidad pretest Sistema de Gestión de Seguridad de la Información

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pretest SGSI	.334	32	.00000

Fuente: elaboración propia

Como se observa en la tabla 19 el valor de Sig. del pretest de la dimensión sistema de gestión de seguridad de la información de la información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, es menor a 0,05, por ello se determina una distribución no normal.

En la tabla 20 se observa como resultado la prueba de normalidad del postest de la influencia de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Tabla 20. Pruebas de normalidad postest Sistema de Gestión de Seguridad de la Información

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Postest SGSI	.172	32	.00000

Fuente: elaboración propia

Como se observa en la tabla 20 el valor de Sig. del postest de la dimensión sistema de gestión de seguridad de la información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, es menor a 0,05, por ello se determina una distribución no normal.

Estadístico descriptivo

En la figura 47, se muestra el pretest de la influencia de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de

información en la Central de Operaciones Policiales de la Región Policial Junín, obteniendo una media de 1,09 y una desviación estándar de 0,296.

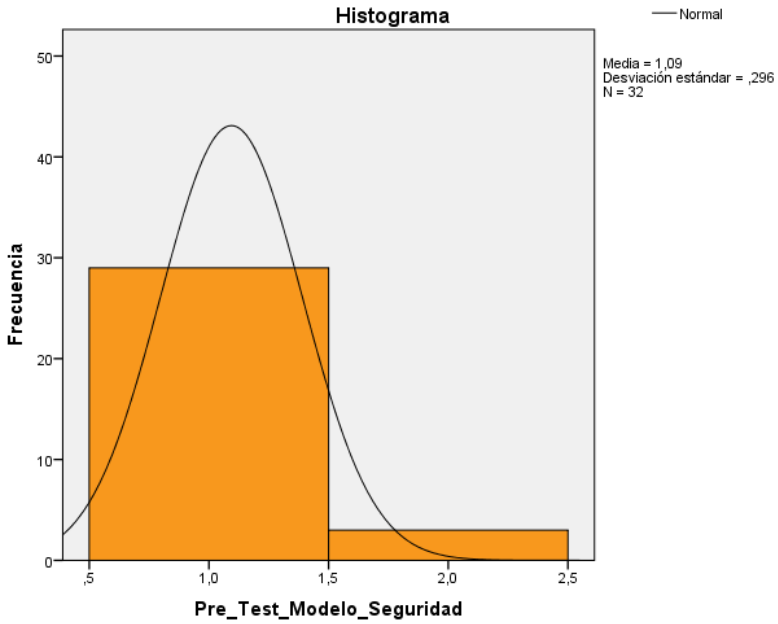


Figura 47. Pretest de la Influencia de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín

Fuente: elaboración propia

En la figura 48, se muestra el Postest de la influencia de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, obteniendo una media de 4,97 y una desviación estándar de 0,177.

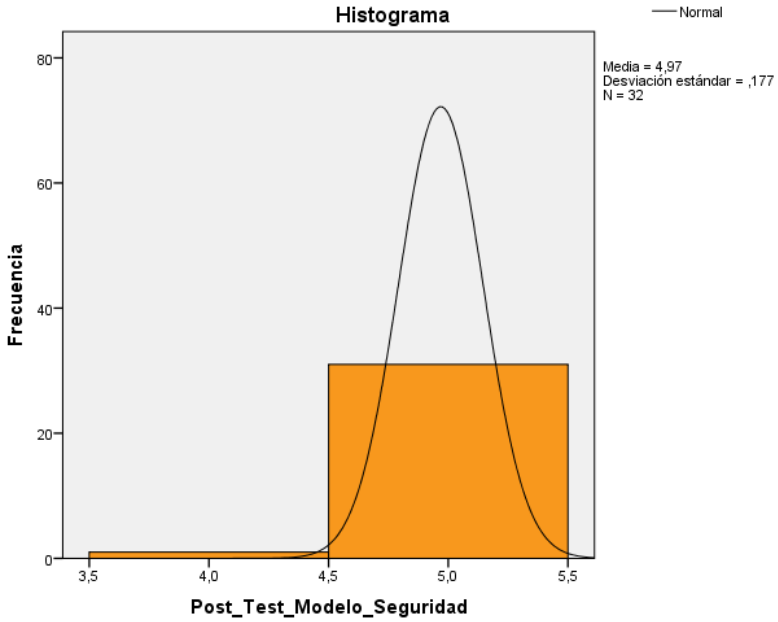


Figura 48. Postest de la Influencia de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín

Fuente: elaboración propia

Tomando los resultados de las figuras anteriores, se observa que existe un aumento considerable en la mitigación de la dimensión sistema de gestión de seguridad de la información, dada la influencia de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, desde 1,09 hasta 4,97.

5.2 Prueba de hipótesis

a. Hipótesis de investigación de la dimensión amenazas

Para contrastar la hipótesis se aplicó la prueba de Wilcoxon, ya que la dimensión amenazas adopta una distribución no normal (Sig. menos a 0.05) en la influencia de un Modelo de Seguridad de la Información para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

En las tablas siguientes, se muestran los resultados de la prueba de Wilcoxon:

Tabla 21. Rangos de la dimensión amenazas

Dimensión Amenazas		N	Rango promedio	Suma de rangos
Pretest Amenazas - Postest Amenazas	Rangos negativos	32[a]	16.50	528.00
	Rangos positivos	0[b]	0.00	0.00
	Empates	0[c]		
	Total	32		

Fuente: elaboración propia

Tabla 22. Estadísticos de prueba de la dimensión amenazas

	Pretest Amenazas - Postest Amenazas
Z	-4,937[b]
Sig. asintótica (bilateral)	.000000793
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Fuente: elaboración propia

H1: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye positivamente en la mitigación de las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, a un nivel de confianza del 95%.

Ho: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 no influye en la mitigación de las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín

De acuerdo a la tabla 22 concluimos que se rechaza la hipótesis nula en vista que el valor de P = Sig. Asintónica (bilateral) es 0.000000793 menor a 0.05, en consecuencia, se acepta que: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye positivamente en la mitigación de las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, a un nivel de confianza del 95%.

En la tabla 23 se muestran los porcentajes comparativos del pretest y postest de la dimensión amenazas.

Tabla 23. Proporciones de medición de la dimensión amenazas

	Pretest		Postest		Total	
	N°	**%**	**N°**	**%**	**N°**	**%**
Probablemente NO	32	100.0%	0	0.0%	32	50.0%
Definitivamente SÍ	0	0.0%	32	100.0%	32	50.0%
Total	**32**	**100.0%**	**32**	**100.0%**	**64**	**100.0%**

Fuente: elaboración propia

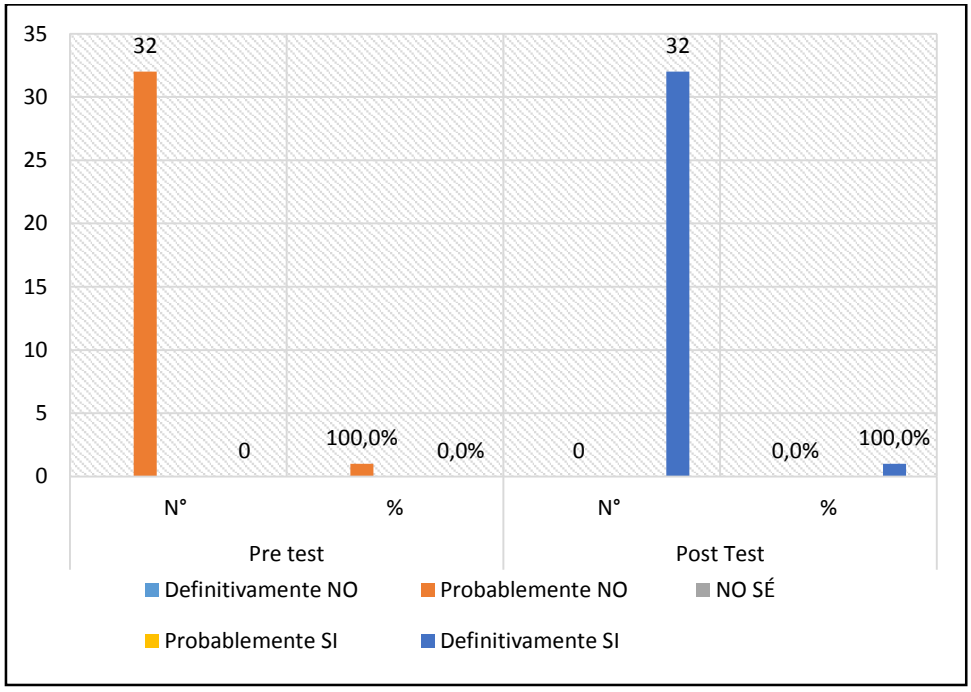


Figura 49. Proporciones de la dimensión Amenazas

Fuente: elaboración propia

b. Hipótesis de investigación de la dimensión vulnerabilidades

Para contrastar la hipótesis se aplicó la prueba de Wilcoxon, ya que la dimensión vulnerabilidades adopta una distribución no normal (Sig. menos a 0.05) en la influencia de un Modelo de Seguridad de la Información para mitigar las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

En las tablas siguientes, se muestran los resultados de la prueba de Wilcoxon:

Tabla 24. Rangos de la dimensión vulnerabilidades

		N	Rango promedio	Suma de rangos
Pretest Vulnerabilidades - Postest Vulnerabilidades	Rangos negativos	32[a]	16.50	528.00
	Rangos positivos	0[b]	0.00	0.00
	Empates	0[c]		
	Total	32		

Fuente: elaboración propia

Tabla 25. Estadísticos de prueba de la dimensión vulnerabilidades

	Pretest Vulnerabilidades - Postest Vulnerabilidades
Z	-5,005[b]
Sig. asintótica (bilateral)	.000000558
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Fuente: elaboración propia

H1: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye positivamente en la mitigación de las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, a un nivel de confianza del 95%.

Ho: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 no influye en la mitigación de las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

De acuerdo a la tabla 25 concluimos que se rechaza la hipótesis nula en vista que el valor de P = Sig. Asintónica (bilateral) es 0.000000558 menor a 0.05, en consecuencia, se acepta que: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye positivamente en la mitigación de las vulnerabilidades a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, a un nivel de confianza del 95%.

En la tabla 26 se muestran los porcentajes comparativos del pretest y postest de la dimensión vulnerabilidades.

Tabla 26. Proporciones de medición de la dimensión vulnerabilidades

	Pretest		Postest		Total	
	N°	**%**	**N°**	**%**	**N°**	**%**
Definitivamente NO	16	50.0%	0	0.0%	16	25.0%
Probablemente NO	16	50.0%	0	0.0%	16	25.0%
NO SÉ	0	0.0%	0	0.0%	0	0.0%
Probablemente SÍ	0	0.0%	0	0.0%	0	0.0%
Definitivamente SÍ	0	0.0%	32	100.0%	32	50.0%
Total	**32**	**100.0%**	**32**	**100.0%**	**64**	**100.0%**

Fuente: elaboración propia

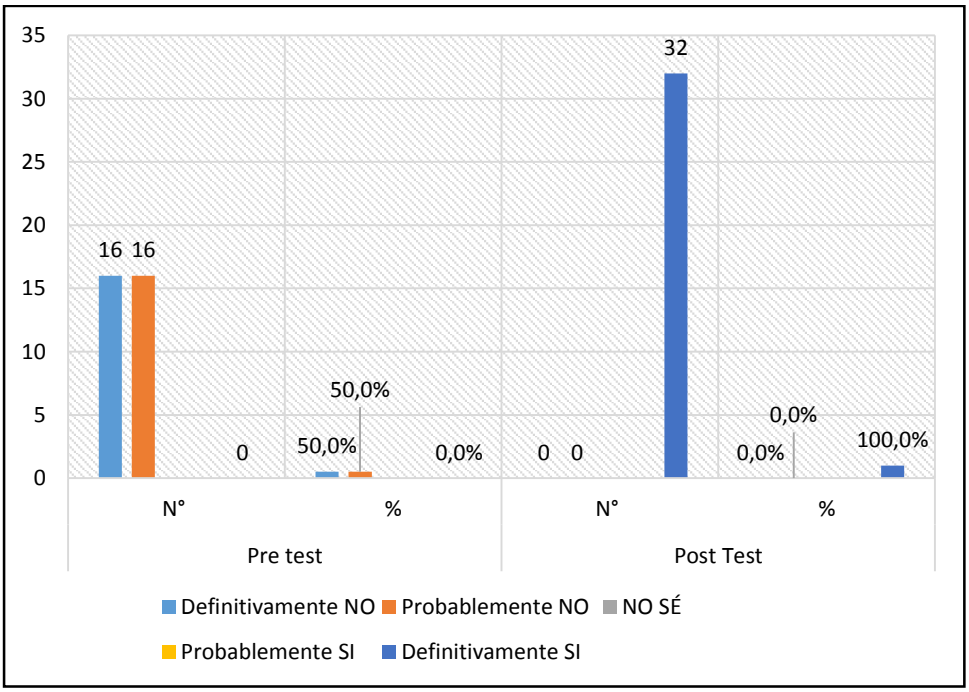


Figura 50. Proporciones de la dimensión Vulnerabilidades

Fuente: elaboración propia

c. Hipótesis de investigación de la dimensión sistema de gestión de seguridad de la información

Para contrastar la hipótesis se aplicó la prueba de Wilcoxon, ya que la dimensión sistema de gestión de seguridad de la información adopta una distribución no normal (Sig. menos a 0.05) en la influencia de un Modelo de Seguridad de la Información para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

En las tablas siguientes, se muestran los resultados de la prueba de Wilcoxon:

Tabla 27. Rangos de la dimensión sistema de gestión de seguridad de la información

		N	Rango promedio	Suma de rangos
Pretest modelo Seguridad - Postest SGSI	Rangos negativos	32[a]	16.50	528.00
	Rangos positivos	0[b]	0.00	0.00
	Empates	0[c]		
	Total	32		

Fuente: elaboración propia

Tabla 28 Estadísticos de prueba de la dimensión gestión seguridad de la información

	Pretest SGSI - Postest SGSI
Z	-5,387[b]
Sig. asintótica (bilateral)	.000000072
a. Prueba de Wilcoxon de los rangos con signo	
b. Se basa en rangos positivos.	

Fuente: elaboración propia

H1: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye positivamente en la mitigación de los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

Ho: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 no influye en la mitigación de los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

De acuerdo a la tabla 28 concluimos que se rechaza la hipótesis nula en vista que el valor de P = Sig. Asintónica (bilateral) es 0.000000072 menor a 0.05, en consecuencia, se acepta que: el establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye positivamente en la mitigación de

los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, a un nivel de confianza del 95%.

En la tabla 29 se muestran los porcentajes comparativos del pretest y postest de la dimensión modelo de seguridad de la información.

Tabla 29. Proporciones de medición de la dimensión SGSI

	Pretest		Postest		Total	
	N°	**%**	**N°**	**%**	**N°**	**%**
Definitivamente NO	29	90.6%	0	0.0%	29	45.3%
Probablemente NO	3	9.4%	0	0.0%	3	4.7%
NO SÉ	0	0.0%	0	0.0%	0	0.0%
Probablemente SÍ	0	0.0%	0	0.0%	0	0.0%
Definitivamente SÍ	0	0.0%	32	100.0%	32	50.0%
Total	**32**	**100.0%**	**32**	**100.0%**	**64**	**100.0%**

Fuente: elaboración propia

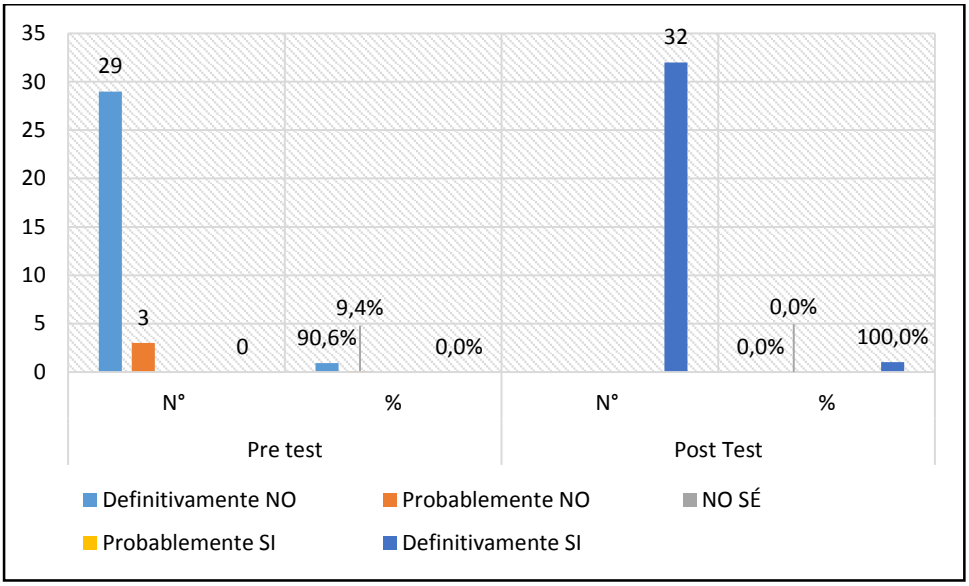


Figura 51. Proporciones de la dimensión SGSI

Fuente: elaboración propia

5.3 Discusión de los resultados

En el presente trabajo de investigación se ha realizado la comparación de los niveles de percepción e incidencias de riesgos, amenazas y vulnerabilidades de los activos de

información pre y postimplementación de un Modelo de Seguridad de la Información basado en la ISO/IEC 27001:2013 para mitigar los riesgos de la información en la Central de Operaciones Policiales de la Región Policial Junín.

a. En la medición general del pretest, alcanzó 1,22 que representa el 24% del nivel de concientización y percepción del personal policial sobre mitigación de riesgos y con la implementación del modelo de seguridad de la información se logró aumentar a 4,96 que representa el 99% el nivel de concientización y percepción del personal policial sobre mitigación de riesgos. Los resultados obtenidos indican que existe un aumento positivo de 3,74 que representa el 75% al realizar la implementación del modelo de seguridad de la información para mitigar los riesgos de los activos de información de la Central de Operaciones Policiales de la Región Policial Junín.

b. En la medición de la dimensión amenazas del pretest, alcanzó 1,30 que representa el 26% del nivel de mitigación de amenazas y con la implementación del modelo de seguridad de la información se logró aumentar a 4.94 que representa el 99% del nivel de mitigación de amenazas. Los resultados obtenidos indican que existe un aumento positivo de 3.64 que representa el 73% al realizar la implementación del modelo de seguridad de la información para mitigar las amenazas de los activos de información de la Central de Operaciones Policiales de la Región Policial Junín. En la realización de la investigación no se encontró antecedentes relacionados al presente estudio.

c. En la medición de la dimensión vulnerabilidades del Pretest, alcanzó 1,50 que representa el 30% del nivel de mitigación de vulnerabilidades y con la implementación del modelo de seguridad de la información se logró aumentar a 5,00 que representa el 100% del nivel de mitigación de vulnerabilidades. Los resultados obtenidos indican que existe un aumento positivo de 3,50 que representa el 70% al realizar la implementación del modelo de seguridad de la información para mitigar las vulnerabilidades de los activos de información de la Central de Operaciones Policiales de la Región Policial Junín. En la realización de la investigación no se encontró antecedentes relacionados al presente estudio.

CONCLUSIONES

Al término del trabajo de investigación se llegó a las siguientes conclusiones:

a. La implementación de un modelo de seguridad de la información basada en la Norma ISO/IEC 27001:2013 influye positivamente en la mitigación de los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, ya que el nivel de concientización y percepción del personal policial sobre mitigación de riesgos preimplementación fue de 1,22 que representa el 24%, y postimplementación fue de 4,96% que representa el 99%, lo que significa un aumento de 3,74% que representa el 75% en el nivel de concientización y percepción del personal policial sobre mitigación de riesgos de los activos de información; con lo que, podemos colegir que la cultura organizacional a nivel de seguridad de la información se ha incrementado en 75%.

b. La implementación de un modelo de seguridad de la información basada en la norma ISO/IEC 27001:2013 influye positivamente en la mitigación de las amenazas de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, ya que el nivel de mitigación de amenazas preimplementación fue de 1,30 que representa el 26%, y el nivel de mitigación de amenazas después de la implementación fue de 4,94 que representa el 99%, lo que significa un aumento de 3,64 que representa el 75% en el nivel de mitigación de amenazas de los activos de información.

c. La implementación de un modelo de seguridad de la información basada en la Norma ISO/IEC 27001:2013 influye positivamente en la mitigación de las vulnerabilidades de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín, ya que el nivel de mitigación de vulnerabilidades preimplementación fue de 1,50 que representa el 30%, y el nivel de mitigación de vulnerabilidades después de la implementación fue de 5,00 que representa el 100%, lo que significa un aumento de 3,50 que representa el 70% en el nivel de mitigación de amenazas de los activos de información.

d. En las encuestas del presente trabajo de investigación se debió utilizar preguntas dicotómicas dados los resultados obtenidos.

e. Se logró incrementar los conocimientos del personal policial, teniendo como resultado personal comprometido y no solo involucrado con la seguridad de la información policial.

f. Finalmente, se logró el compromiso de la Dirección de la VI Macrorregión Junín, Pasco y Huancavelica de la Policía Nacional del Perú, en temas de seguridad de la información.

RECOMENDACIONES

- Se recomienda ampliar el alcance de la presente investigación orientada exclusivamente a la plataforma integrada de Información e Inteligencia denominada PI3-CHASKA (aplicación web), de reciente implementación en la Centrales de Operaciones Policiales a nivel nacional; asimismo, ampliar el alcance de las políticas de seguridad del presente a las Regiones Policiales de Huancavelica y Pasco, como primera fase y alternativa para una posible obtención de la certificación internacional en calidad y seguridad de la información.
- Al director de la VI Macrorregión Junín, Huancavelica y Pasco de la Policía Nacional del Perú con sede en Huancayo, se recomienda gestionar la implementación de nuevas tecnologías que permitan optimizar el tratamiento de los datos sensibles y fotografías de detenidos y/o intervenidos, como primer paso, con el uso exclusivo del correo institucional.
- Se recomienda afianzar los cursos de informática básica y ética policial a cargo de profesionales capacitados en seguridad de la información para los alumnos en proceso de formación en las Escuelas de Educación Superior Técnica Profesional de la Policía Nacional del Perú.
- Se recomienda continuar con las campañas de sensibilización al personal policial de la Central de Operaciones Policiales de la Región Policial Junín.
- Se recomienda realizar jornadas periódicas de capacitación y sensibilización al personal policial de la Oficina de Inteligencia Territorial Huancayo en temas de seguridad de la información y ética policial.
- Se recomienda realizar posteriormente una auditoría interna al SGSI, para determinar el estado de los controles de seguridad que fueron implementados.
- Se sugiere fortalecer el comité de seguridad de la información para optimizar el SGSI.
- Se sugiere realizar la actualización de los equipos de cómputo, a fin de conservar e incrementar la calidad del servicio que prestan y establecer las disposiciones pertinentes para el acceso a áreas críticas (oficina) y uso de equipos cuya misión es crítica (información clasificada), así como para el registro del tráfico de personal en dichas áreas, teniendo en cuenta situaciones de emergencia o de urgencia manifiesta.

REFERENCIAS BIBLIOGRÁFICAS

27001 ACADEMY. 27001 ACADEMY . [En línea] [Citado el: 19 de octubre de 2016.] http://advisera.com/27001academy/es/.

27001:2014, NORMA TÉCNICA PERUANA NTP-ISO/IEC. (2014). PECERT Sistema de Coordinacion de la Administracion Pública. *Coordinación de Emergencias en Redes Teleinformáticas.* [En línea] 20 de noviembre de 2014. [Citado el: 24 de octubre de 2016.] http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf.

Aguirre Cardona, Juan David y Aristizábal Betancourt, Catalina. (2013). Biblioteca e Información Científica de la Universidad Tecnológica de Pereira. [En línea] 2013. [Citado el: 20 de octubre de 2016.] http://repositorio.utp.edu.co/dspace/handle/11059/4117. T005.8 A284;6310000106927 F2579.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). Administración Electrónica del Gobierno de España. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información 3.0.* [En línea] octubre de 2012. [Citado el: 23 de octubre de 2016.] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_*Magerit*.html#.WAzPOdJ97IU. 630-12-171-8.

Fernández Peñaloza, David Aurelio y Pacheco Vargas, Oscar Alexis. (2014). Repositorio Acádemico Universidad San Martín de Porres. [En línea] 08 de febrero de 2014. [Citado el: 2016 de octubre de 2016.] www.repositorioacademico.usmp.edu.pe/handle/usmp/1470.

General, Policía Nacional del Perú-Estado Mayor. (2016). *Manual de Documentación Policial.* Lima.

Justino Salinas, Zully Isabel. (2015). Repositorio Digital de Tesis PUCP. [En línea] 04 de junio de 2015. [Citado el: 20 de octubre de 2016.] http://tesis.pucp.edu.pe/repositorio/handle/123456789/6045. 2310-8894.

Luis Gómez Fernández, y Ana Andrés Álvarez. (2009). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* Madrid : AENOR España, 2009. 978-84-8143-602-0.

Mataix Lorda, Mariano y Mataix Hidalgo, Miguel. (1999). Diccionario de electrónica, informática y energía nuclear. [En línea] 1999. [Citado el: 28 de diciembre de 2016.] 978-84-7978-411-9.

Pallas Mega, Gustavo. (2009). Metodología de implantación de un SGSI en un grupo empresarial jerárquico. [En línea] 2009. [Citado el: 21 de octubre de 2016.] https://www.colibri.udelar.edu.uy/handle/123456789/2954.

ANEXOS

ANEXO A. MATRIZ DE CONSISTENCIA

TÍTULO: Modelo de seguridad de la información basado en la ISO/IEC 27001:2013 para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
General	**General**	**General**	**Variable X**			
¿Cuál es la influencia de un modelo de seguridad de la información basado en la ISO 27001 para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín?	Determinar la influencia de un modelo de seguridad de la información basado en la ISO 27001 para mitigar los riesgos a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.	El Establecimiento de un modelo para la seguridad de la información basado en la ISO 27001 influye significativamente en mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.	**Modelo de seguridad de la información basada en la ISO 27001** (Guía de Luís Gómez Fernández y Ana Andrés Álvarez)	Sistema de Gestión de Seguridad de la Información	1. Confidencialidad 2. Integridad 3. Disponibilidad	**TIPO DE INVESTIGACIÓN** Aplicada **NIVEL DE INVESTIGACIÓN** Explicativo
Específicos	**Específicos**	**Específicos**	**Variable Y**			

¿Cuál es la influencia de un modelo de seguridad de la información basado en la ISO 27001 para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín?	Establecer un modelo de seguridad de la información y determinar su influencia para mitigar las amenazas a los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.	El establecimiento de un modelo de seguridad de la información influye directamente en mitigar las amenazas de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín	**Riesgo de los activos de información** (Análisis y gestión de riesgos implementando la metodología *Magerit* versión 3.0-Instituto Nacional de Ciberseguridad del Gobierno de España)	Amenazas	4. Indisponibilidad del personal 5. Fuga de información 6. Introducción de falsa información 7. Alteración de la información 8. Corrupción de la información 9. Destrucción de información.	
¿Cuál es la influencia de un modelo de seguridad de la información basado en la ISO 27001 para mitigar las vulnerabilidades de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín?	Establecer un modelo de seguridad de la información y determinar su influencia para mitigar la vulnerabilidad de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.	El establecimiento de un modelo de seguridad de la información influye directamente en mitigar las vulnerabilidades de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.		Vulnerabilidades	10. Incidentes de seguridad de la Información 11. Abuso de privilegios de acceso 12. Acceso no autorizado 13. Seguridad física y del entorno 14. Mantenimiento de sistemas	

ANEXO B. CUADRO DE OPERACIONALIZACIÓN DE VARIABLES			
VARIABLES	**DIMENSIONES**	**INDICADORES**	**PREGUNTAS**
Modelo de seguridad de la información basada en la ISO/IEC 27001:2013	Sistema de Gestión de Seguridad de la Información	Confidencialidad	1. En su opinión, ¿existe un acuerdo de confidencialidad de la información a la que se accede? 2. En su opinión, ¿es aceptable compartir información textual o imágenes sobre operaciones policiales de carácter confidencial sabiendo que se trata de un hecho de fuga de información y puede constituirse en delito de infidencia?
		Integridad	3. En su opinión, ¿es aceptable recibir documentos de texto digitales vía correo electrónico sobre operaciones policiales y/o disposiciones de comando de carácter reservado sin verificar su procedencia y/o fuente? 4. En su opinión, ¿es aceptable recibir documentos de texto digitales (notas informativas o notas de información) vía correo electrónico sobre hechos que se suscitan en la jurisdicción de la región Junín sin verificar su procedencia y/o fuente?
		Disponibilidad	5. En su opinión, ¿se dispone de una clasificación de la información según la criticidad de la misma? 6. En su opinión, ¿existe un responsable de los activos? 7. En su opinión, ¿existen procedimientos para clasificar la información?

Riesgos de los activos de información	Amenazas	Indisponibilidad del personal	8. En su opinión, ¿existen documentos de políticas de seguridad de los Sistemas de Información en la Central de Operaciones Policiales (Ceopol) y Oficina de Inteligencia (Ofinte) de la Región Policial Junín? 9. En su opinión, ¿existe normativa relativa a la seguridad de los Sistemas de Información en la Ceopol y Ofinte? 10. En su opinión, ¿existen procedimientos relativos a la seguridad de los Sistemas de Información en la Ceopol y Ofinte? 11. En su opinión, ¿existe un responsable de las políticas, normas y procedimientos en Seguridad Informática? 12. En su opinión, ¿existen mecanismos para la comunicación a los usuarios de las normas? 13. En su opinión, ¿existen controles regulares para verificar la efectividad de las políticas? 14. En su opinión, ¿existe un inventario de activos actualizado? 15. En su opinión ¿el inventario contiene activos de datos, software, equipos y servicios?
		Fuga de información	16. En su opinión, ¿existen roles y responsabilidades definidas para las personas implicadas en la seguridad? 17. En su opinión, ¿un responsable encargado de evaluar la adquisición y cambios de los Sistemas de Información en la Ceopol y Ofinte? 18. En su opinión, ¿la dirección y la Ofitic de la Región Policial Junín participan en temas de seguridad? 19. En su opinión, ¿existen programas de formación en seguridad informática para el personal PNP?
		Introducción de falsa información	20. En su opinión, ¿es inútil tener documentos físicos de la información que se recibe, centraliza, genera y procesa? 21. En su opinión, ¿es inútil configurar pantallas de bloqueo en los equipos de cómputo dado el tiempo de inactividad? 22. En su opinión ¿sería inútil mantener un registro de los

			documentos de información que se formulan y remiten a los distintos niveles de comando de la Policía Nacional del Perú?
		Alteración de la información	23. En su opinión, ¿informan a los usuarios de las vulnerabilidades observadas o sospechosas? 24. En su opinión, ¿son nulos los errores involuntarios en el uso de las aplicaciones informáticas? 25. En su opinión, ¿existe un proceso disciplinario de la seguridad de la información, implantado?
		Corrupción de la información	26. En su opinión, ¿se tienen definidas las responsabilidades y roles de seguridad? 27. En su opinión, ¿se tiene en cuenta la seguridad en la selección del personal? 28. En su opinión, ¿se plasman las condiciones de confidencialidad y responsabilidad al ingresar a laborar a la Ceopol y Ofinte? 29. En su opinión, ¿se imparte la formación y/o capacitación adecuada de seguridad y tratamiento de activos?
		Destrucción de información	30. En su opinión, ¿es inútil mantener un registro de pérdidas de datos o información en la Central de Operaciones Policiales de la Región Policial Junín? 31. En su opinión, ¿existe algún control en las redes para compartir archivos digitales? 32. ¿Existen medidas de seguridad en el uso del correo electrónico?
	Vulnerabilidades	Incidentes de seguridad de la Información	33. En su opinión, ¿existe un canal y procedimientos claros a seguir en caso de incidente de seguridad? 34. En su opinión, ¿están establecidas las responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad? 35. En su opinión, ¿se comunican las debilidades de seguridad? 36. En su opinión, ¿existen definidas las responsabilidades antes

			de un incidente? 37. En su opinión, ¿existe un procedimiento formal de respuesta? 38. En su opinión, ¿existe un marco de planificación para la continuidad del negocio?
		Abuso de privilegios de acceso	39. En su opinión, ¿se tiene en cuenta el cumplimiento de la legislación policial? 40. En su opinión, ¿existe una revisión de la política de seguridad y de la conformidad técnica?
		Acceso no autorizado	41. En su opinión, ¿existe el uso de passwords? 42. En su opinión, ¿existe una política de uso de los servicios de red?
		Seguridad física y del entorno	43. En su opinión, ¿falta un perímetro de seguridad física eficiente (una pared, puerta con llave, control de acceso físico) en la Ceopol y Ofinte? 44. En su opinión, ¿existen controles de entrada para protegerse frente al acceso de personal no autorizado? 45. En su opinión, ¿un área vulnerable ha de estar cerrada, aislada y protegida de eventos naturales? 46. En su opinión, ¿existen protecciones frente a fallos en la alimentación eléctrica?
		Mantenimiento de sistemas	47. En su opinión, ¿se realiza mantenimiento y control en las vulnerabilidades de los equipos? 48. En su opinión, ¿están actualizados los sistemas operativos, antivirus, aplicaciones y programas de los equipos de cómputo de la Ceopol y Ofinte? 49. En su opinión, ¿la oficina de la Ceopol y Ofinte cuentan con hardware o equipamiento apropiado?

ANEXO C. CUESTIONARIO DE EVALUACIÓN AL PERSONAL POLICIAL

Universidad Continental

ENCUESTA EN SEGURIDAD DE LA INFORMACIÓN PARA APOYAR LA TESIS TITULADA:

"MODELO DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO/IEC 27001:2013 PARA MITIGAR LOS RIESGOS DE LOS ACTIVOS DE INFORMACIÓN EN LA CENTRAL DE OPERACIONES POLICIALES Y OFICINA DE INTELIGENCIA DE LA REGIÓN POLICIAL JUNÍN"

OBJETIVO:
Realizar una evaluación técnica informática y obtener un diagnóstico general y situación actual de la seguridad informática en la Central de Operaciones Policiales y Oficina de Inteligencia de la Región Policial Junín, para verificar las falencias y proponer controles y políticas de seguridad en base a los resultados y recomendaciones obtenidas y minimizar en el futuro su ocurrencia, además obtener una forma de prevención para el tratamiento adecuado de datos y el cuidado de la información policial.

Estimado colega, por favor conteste las siguientes preguntas de manera honesta y concreta, marcando la respuesta que considere correcta.

Subunidad:

- ☐ CEOPOL
- ☐ OFINTE

Grado:

- ☐ Gral. PNP
- ☐ Crnl. PNP
- ☐ Cmdte. PNP
- ☐ May. PNP
- ☐ Cap. PNP
- ☐ Tnte. PNP
- ☐ Alfz. PNP
- ☐ SS. PNP
- ☐ SB. PNP
- ☐ ST1. PNP
- ☐ ST2. PNP
- ☐ ST3. PNP
- ☐ S1. PNP
- ☐ S2. PNP
- ☐ S3. PNP

Fecha: ____/11/2016

CUESTIONARIO:

Nº	Pregunta	Definitivamente NO	Probablemente no	No sé	Probablemente SÍ	Definitivamente SÍ
		👎	☹	😐	☺	👍
CONFIDENCIALIDAD						
01	En su opinión, ¿existe un acuerdo de confidencialidad de la información a la que se accede?	👎	☹	😐	☺	👍
02	En su opinión, ¿es aceptable compartir información textual o imágenes sobre operaciones policiales de carácter confidencial sabiendo que se trata de un	👎	☹	😐	☺	👍

	hecho de fuga de información y puede constituirse en delito de infidencia?					
INTEGRIDAD						
03	En su opinión, ¿es aceptable recibir documentos de texto digitales vía correo electrónico sobre operaciones policiales y/o disposiciones de comando de carácter reservado sin verificar su procedencia y/o fuente?					
04	En su opinión, ¿es aceptable recibir documentos de texto digitales (notas informativas o notas de información) vía correo electrónico sobre hechos que se suscitan en la jurisdicción de la región Junín sin verificar su procedencia y/o fuente					
DISPONIBILIDAD						
05	En su opinión, ¿se dispone de una clasificación de la información según la criticidad de la misma?					
06	En su opinión, ¿existe un responsable de los activos?					
07	En su opinión, ¿existen procedimientos para clasificar la información?					
INDISPONIBILIDAD DEL PERSONAL						
08	En su opinión, ¿existen documentos de políticas de seguridad de los Sistemas de Información en la Central de Operaciones Policiales (Ceopol) y Oficina de Inteligencia (Ofinte) de la Región Policial Junín?					
09	En su opinión, ¿existe normativa relativa a la seguridad de los Sistemas de Información en la Ceopol y Ofinte?					
10	En su opinión, ¿existen procedimientos relativos a la seguridad de los Sistemas de Información en la Ceopol y Ofinte?					
11	En su opinión, ¿existe un responsable de las políticas, normas y procedimientos en Seguridad Informática?					
12	En su opinión, ¿existen mecanismos para la comunicación a los usuarios de las normas?					
13	En su opinión, ¿existen controles regulares para verificar la efectividad de las políticas?					
14	En su opinión, ¿existe un inventario de activos actualizado?					
15	En su opinión ¿el inventario contiene activos de datos, software, equipos y servicios?					

FUGA DE INFORMACIÓN						
16	En su opinión, ¿existen roles y responsabilidades definidas para las personas implicadas en la seguridad?					
17	En su opinión, ¿un responsable encargado de evaluar la adquisición y cambios de los Sistemas de Información en la Ceopol y Ofinte?					
18	En su opinión, ¿la dirección y la Ofitic de la Región Policial Junín participan en temas de seguridad?					
19	. En su opinión, ¿existen programas de formación en seguridad informática para el personal PNP?					
INTRODUCCIÓN DE FALSA INFORMACIÓN						
20	En su opinión, ¿es inútil tener documentos físicos de la información que se recibe, centraliza, genera y procesa?					
21	En su opinión, ¿es inútil configurar pantallas de bloqueo en los equipos de cómputo dado el tiempo de inactividad?					
22	En su opinión ¿sería inútil mantener un registro de los documentos de información que se formulan y remiten a los distintos niveles de comando de la Policía Nacional del Perú?					
ALTERACIÓN DE LA INFORMACIÓN						
23	En su opinión, ¿informan a los usuarios de las vulnerabilidades observadas o sospechosas?					
24	En su opinión, ¿son nulos los errores involuntarios en el uso de las aplicaciones informáticas?					
25	En su opinión, ¿existe un proceso disciplinario de la seguridad de la información, implantado?					
CORRUPCIÓN DE LA INFORMACIÓN						
26	En su opinión, ¿se tienen definidas las responsabilidades y roles de seguridad?					
27	En su opinión, ¿se tiene en cuenta la seguridad en la selección del personal?					
28	En su opinión, ¿se plasman las condiciones de confidencialidad y responsabilidad al ingresar a laborar a la Ceopol y Ofinte?					
29	En su opinión, ¿se imparte la formación y/o capacitación adecuada de seguridad y tratamiento de activos?					

DESTRUCCIÓN DE LA INFORMACIÓN						
30	En su opinión, ¿es inútil mantener un registro de pérdidas de datos o información en la Central de Operaciones Policiales de la Región Policial Junín?					
31	En su opinión, ¿existe algún control en las redes para compartir archivos digitales?					
32	¿Existen medidas de seguridad en el uso del correo electrónico?					
INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN						
33	En su opinión, ¿existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?					
34	En su opinión, ¿están establecidas las responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?					
35	En su opinión, ¿se comunican las debilidades de seguridad?					
36	En su opinión, ¿existen definidas las responsabilidades antes de un incidente?					
37	En su opinión, ¿existe un procedimiento formal de respuesta?					
38	En su opinión, ¿existe un marco de planificación para la continuidad del negocio?					
ABUSO DE PRIVILEGIOS DE ACCESO						
39	En su opinión, ¿se tiene en cuenta el cumplimiento de la legislación policial?					
40	En su opinión, ¿existe una revisión de la política de seguridad y de la conformidad técnica?					
ACCESO NO AUTORIZADO						
41	En su opinión, ¿existe el uso de passwords?					
42	En su opinión, ¿existe una política de uso de los servicios de red?					
SEGURIDAD FÍSICA Y DEL ENTORNO						
43	En su opinión, ¿falta un perímetro de seguridad física eficiente (una pared, puerta con llave, control de acceso físico) en la Ceopol y Ofinte?					

44	En su opinión, ¿existen controles de entrada para protegerse frente al acceso de personal no autorizado?					
45	En su opinión, ¿un área vulnerable ha de estar cerrada, aislada y protegida de eventos naturales?					
46	En su opinión, ¿existen protecciones frente a fallos en la alimentación eléctrica?					
MANTENIMIENTO DE SISTEMAS						
47	En su opinión, ¿se realiza mantenimiento y control en las vulnerabilidades de los equipos?					
48	En su opinión, ¿están actualizados los sistemas operativos, antivirus, aplicaciones y programas de los equipos de cómputo de la Ceopol y Ofinte?					
49	En su opinión, ¿la oficina de la Ceopol y Ofinte cuentan con hardware o equipamiento apropiado?					

ANEXO D. ENTREGABLES DEFINIDOS POR LA NORMA ISO/IEC 27001

Central de Operaciones Policiales de la Región Policial Junín

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PROCEDIMIENTO PARA EL CONTROL Y REGISTRO DE DOCUMENTOS

Versión: 01

Código	**:**	**CPCRD**
Fecha	**:**	**06/12/2016**
Creado por	**:**	**Jean Carlo Zacarias Villafranca**
Aprobado por	**:**	**Jefe de Estado Mayor-OFIPLAAD**
Nivel de Confidencialidad	**:**	**Intimo / Intermedio / Superficial**

CONTENIDO

PROCEDIMIENTO PARA EL CONTROL DE DOCUMENTOS Y REGISTROS

1. OBJETIVOS Y USUARIOS

1.1. Objetivo general

Establecer los procedimientos, principios y normas para la elaboración y control de los documentos y registros asociados al Sistema de Gestión de Seguridad de la Información de la Central de Operaciones Policiales de la Región Policial Junín.

1.2. Objetivos específicos

- Definir los procedimientos a seguir en la cadena de producción documental del Sistema de Gestión de Seguridad de la Información de la Central de Operaciones Policiales de la Región Policial Junín.
- Viabilizar el manejo de la documentación del Sistema de Gestión de Seguridad de la Información de la Central de Operaciones Policiales de la Región Policial Junín, reflejando el fortalecimiento de la identidad institucional.
- Permitir un control eficaz y eficiente de la información y documentación, por medio de actividades de seguimiento, control y verificación.
- Permitir la difusión a todo el personal policial que forma parte del Sistema de Gestión de Seguridad de la Información de la Central de Operaciones Policiales de la Región Policial Junín, a fin de que tengan conocimiento de la elaboración y control de los documentos que se generan.

2. ALCANCE

Se aplica a todos los documentos que soportan y componen el Sistema de Gestión de la Seguridad de la Información (SGSI) de la de la Central de Operaciones Policiales de la Región Policial Junín, de conformidad a la norma ISO/IEC 27001:2013.

3. PROCEDIMIENTO DE CONTROL DE DOCUMENTOS INTERNOS

Se establece el procedimiento con el fin de determinar las actividades concernientes a la elaboración, aprobación, actualización, distribución y conservación de los documentos de la Central de Operaciones Policiales de la Región Policial Junín, a fin de disponer y obtener la información de manera ágil y eficiente, contribuyendo a la correcta preservación de la documentación del Sistema de Gestión del Sistema de Información.

Los parámetros a cumplir en la elaboración de los documentos son los siguientes:

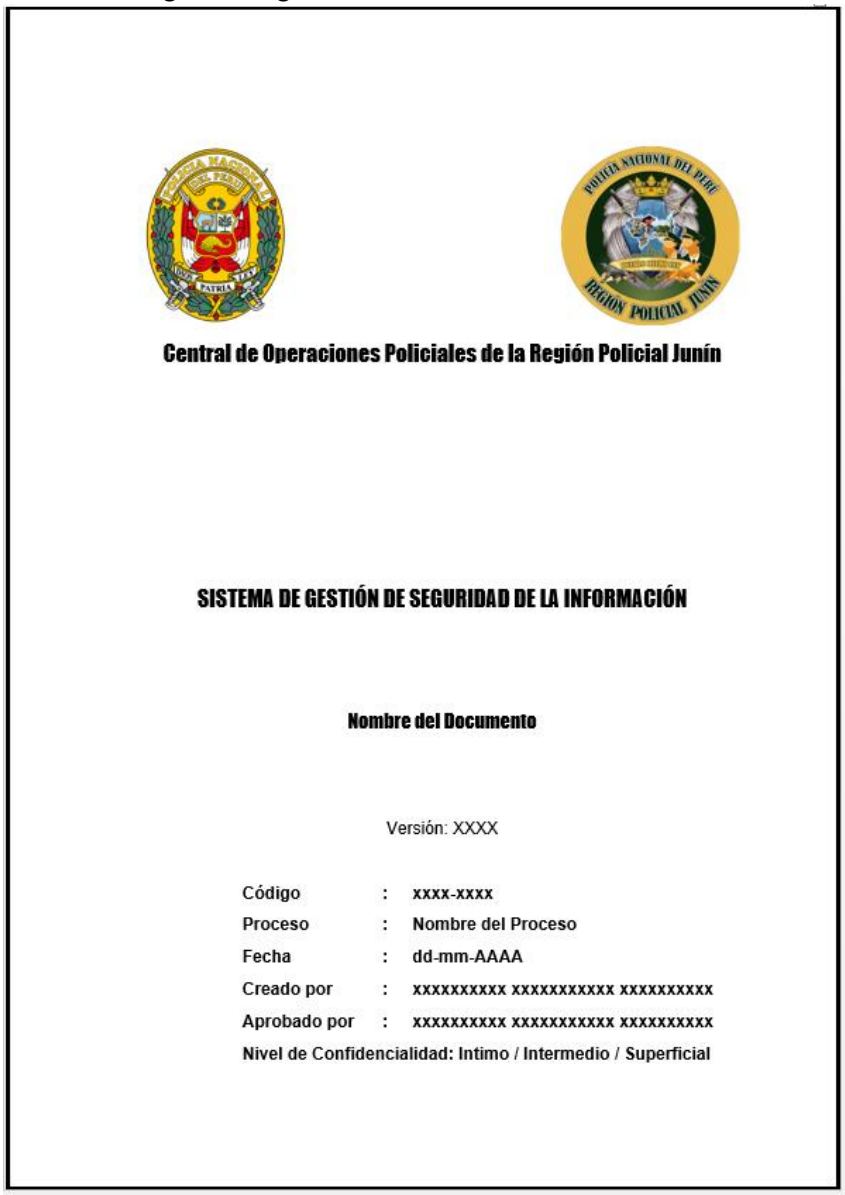
3.1 Formatos y cuerpo de los documentos

Los documentos del SGSI, como manuales, instructivos, guías, informes, protocolos y programas se deben elaborar en papel bond blanco, tamaño A4, con peso de 60 a 80 gr., con márgenes superior e izquierda 3.5 cm,

inferior y derecha 2.0 cm, encabezado 3.0 cm, pie de página 2.0 cm, fuente tipográfica Arial tamaño 12.

3.2 Portada

El texto de la portada se escribe en fuente tipográfica Arial, tamaño 12, el nombre del documento en fuente tipográfica *Impact*, tamaño 16, negrita y alineado en el centro. La estructura de la portada debe encontrarse como se indica en la siguiente gráfica:



En la parte superior del documento, seis (6) interlineaciones bajo el margen superior, a ambos lados, encontramos el logo símbolo de la Policía Nacional del Perú y Región Policial Junín compuesto por el escudo de la Policía Nacional del Perú y Región Policial Junín. Aprobado mediante Acuerdo del Ministerio del Interior el 30 de agosto del año 1988. Los escudos deben tener un tamaño de 4.5 cm de alto por 3.66 de ancho y 4.5 cm de alto por 4.55 de ancho respectivamente, el nombre debe estar escrito

con fuente *Impact* y se escribirá cumpliendo el Manual de Identidad del siguiente modo:
Central de Operaciones Policiales de la Región Policial Junín
en tamaño de fuente 16 negrita.
Seis (6) interlineaciones bajo los logos símbolos encontraremos los datos requeridos por el documento. Estos datos son: el texto **Sistema de Gestión de Sistemas de Información** en fuente *Impact* negrita tamaño 16.
Tres (3) interlineaciones después, encontramos el nombre del documento en fuente *Impact* negrita tamaño 14.
Tres (3) interlineaciones bajo el nombre del documento, se encuentra la versión del documento, cinco (3) interlineaciones después se encuentra el código que identifica al documento, una (1) interlineación más abajo se registra el nombre del proceso del documento, seguido de la fecha de vigencia del documento, nombre del que formula, aprueba y nivel de confidencialidad.
Estos últimos datos se registran con fuente Arial negrita con tamaño 12. La interlineación de la portada debe ser sencilla, tenga en cuenta el Manual de Documentación Policial R.D. N° 776-2016-DIRGEN/EMG-PNP del 27JUL16.

3.3 Encabezado

El encabezado de los documentos del SGSI se encuentra en todas las hojas que conforman el documento, excepto en la portada, deben estar registrados en fuente tipográfica Arial tamaño 9 y debe tener el siguiente contenido:

- **Extremo izquierdo**
  Se encuentra el escudo de la Policía Nacional del Perú, debe tener un tamaño de 2.0 cm de alto por 1.63 de ancho.
- **Centro**
  Se registrarán los nombres de la dependencia o proceso, de este modo, los documentos de uso general llevarán el texto “Sistema de Gestión de Seguridad de Información”, los de uso por proceso llevarán el nombre que los identifica y los de uso por dependencia llevarán el nombre de la misma.
- **Extremo derecho**
  Se encuentra el escudo de la Región Policial Junín, debe tener un tamaño de 2.0 cm de alto por 2.02 de ancho.
- **Extremo medio derecho**
  Se deben registrar los siguientes datos:
  - **Código**, conjunto de caracteres asignados por la Unidad de Archivo y Correspondencia, que se determina de acuerdo al proceso y tipo de documento de acuerdo al siguiente orden:

    Documentos de uso general
    Los documentos que son aplicables a toda la institución se codificarán de la siguiente manera:

Los primeros cuatro dígitos tienen las iniciales del Sistema de Gestión de Seguridad de la Información (SGSI), los dos siguientes al tipo documental, seguidos de su consecutivo.

Documentos de uso por procesos
Los documentos que son aplicables por proceso se codificarán así: Las tres primeras letras corresponden al proceso, los dos siguientes al tipo de documento y los dos últimos al consecutivo.

Documentos de uso por dependencia
Los documentos que son sustantivos de las funciones de cada dependencia y no son aplicables a otras, se codificarán de la siguiente manera: los tres primeros dígitos corresponden a la dependencia, los tres siguientes al proceso, los dos siguientes al tipo de documento y los dos últimos al consecutivo.
Nota: los códigos que se asignan a los documentos asociados al SGSI corresponden al Instructivo de Codificación de Documentos, código SGSI-IN-01 y se registran el Listado Maestro de Documentos Internos, código SGSI-FR-17.

- **Página**: debe evidenciar el número de la página actual frente al número total de páginas. Por ejemplo: **1 de 11**.
- **Versión**: corresponde al número de publicaciones aceptadas del documento.
- **Vigencia a partir de**: se refiere a la fecha de aceptación de la versión del documento, la cual se registra de acuerdo al sistema internacional: año, mes, día; separados por un guion (xx-xx-xxxx), de este mismo modo se registrará en el cierre y en el control de cambios.

Nota: dado el tamaño variable de los formatos de la institución policial, no se estipula un tamaño exacto de encabezado, pero se debe respetar los requerimientos del Manual de Documentación Policial. El tipo de letra de los datos registrados en el centro e izquierda del encabezado deben ser en fuente tipográfica Arial, negrita, mayúscula sostenida para los nombres e inicial para los datos, tamaño de fuente 9.

3.4 Cierre y pie de página del documento

Los datos contenidos en el cierre del documento nos permiten verificar quién lo creó, quién lo revisó y quién lo aprobó, de este modo se identifican los responsables del documento.

- **Elaborado por**: en esta casilla se registra el responsable de la elaboración o creación del documento, o autor del mismo.
- **Revisado por**: en esta casilla se registra el asesor del proceso y representante del Estado Mayor para el Sistema Integrado de Gestión de Calidad.

- **Aprobado por**: en esta casilla se registra el nombre del líder del proceso, quien es el responsable de la verificación final del contenido de los documentos. Dado el valor técnico de los documentos, es necesario que aquellos que lo posean, se aprueben por el Jefe de Estado Mayor o Jefe de la Oficina de Planeamiento Administrativo del Estado Mayor de la región Policial Junín.

Cada una de estas casillas debe especificar cargo, nombre, firma y fecha en su respectiva columna. Cabe resaltar que el uso de firmas digitales está autorizado. La fuente tipográfica a utilizar en el cierre del documento es Arial tamaño 9, negrita y mayúscula inicial.

Gráfica del cierre del documento

	ELABORADO POR	**REVISADO POR**	**APROBADO POR**
CARGO	Responsable del Procedimiento	Representante del Estado Mayor	Líder del proceso
NOMBRE	Jean Carlo Zacarias Villafranca		
FIRMA			
FECHA			

3.5 Contenido del documento

El contenido del documento debe ser claro, conciso, evitando redundancias y errores gramaticales y ortográficos, teniendo en cuenta que los documentos son la carta de presentación de la institución policial. Por razones de variación en los formatos, se recomienda que la fuente sea Arial, el tamaño de fuente depende del tipo y tamaño del formato.

3.6 Control de cambios

El Control de Cambios consiste en una tabla que permite llevar control sobre las solicitudes de modificación del documento, cuántas veces se han llevado a cabo las modificaciones y por qué se realizó. Esta tabla se debe incluir al final del documento, bajo los datos de elaboración y generar un formato denominado Control de Cambios, código SGSI-FR-19. Los datos contenidos en el Control de Cambios son los siguientes:

Versión: corresponde al número de versiones existentes del mismo documento. Cabe indicar que la última versión es la que se toma en cuenta para difusión.

Fecha de aprobación: corresponde a la fecha de aprobación de la versión que se encuentra vigente.

Descripción del cambio: referencia de la razón por la cual fue modificado el documento.

Gráfica del control de cambios

CONTROL DE CAMBIOS		
VERSIÓN N°	**FECHA DE APROBACIÓN**	**DESCRIPCIÓN DEL CAMBIO**

Nota: los datos de cierre del documento y control de cambios únicamente se registran en los documentos y no en los registros o libros de registros.

4. PROCEDIMIENTO DE CONTROL DE DOCUMENTOS EXTERNOS

Procedimiento establecido con el fin de establecer controles para la identificación y control de los documentos externos que afectan al SGSI, con el fin de disponer de la información de manera adecuada, evitando el uso de documentos obsoletos, contribuyendo al mejoramiento continuo de los Procesos y Procedimientos en la Institución.

Los Documentos Externos que afectan al SGSI son:

- Documentos Legales, entre ellos, la Constitución Política del Perú, Leyes, Acuerdos, Decretos y Códigos Peruanos de diferente naturaleza.
- Manuales de funcionamiento, directrices y demás documentos que se relacionen con el manejo de equipos propios de la Central de Operaciones Policiales de la Región Policial Junín.
- Documentos generados, por otras instituciones y que tengan relación directa con las actividades y funciones realizadas por las diferentes dependencias.
- Documentos implementados, por una dependencia pero que son generados por otra, como, por ejemplo, las Resoluciones Ministeriales o las Resoluciones Directorales que se aplican a varias regiones policiales.
- Los documentos externos se identifican con el sello de copia controlada del SGSI y se incluyen en el Listado Maestro de Documentos Externos SGSI-FR-18. Los líderes de los procesos deben reportar, al Asesor de Seguridad asignado, los documentos externos que utilicen y que se hayan modificado o actualizado en cumplimiento de sus funciones para la actualización del Listado Maestro de Documentos Externos. A su vez, el asesor debe reportar dentro de los 5 últimos días de cada mes los cambios realizados a la Unidad de Archivo y Correspondencia para consolidar el Listado Maestro de Documentos Externos de la Institución Policial.

5. PROCEDIMIENTO DE CONTROL DE REGISTROS

Procedimiento que establecen las actividades necesarias para la identificación, almacenamiento, conservación, recuperación, retención y disposición de los registros que se generan en cumplimiento de las funciones y procedimientos establecidos por el SGSI.

5.1 Diligenciamiento

El diligenciamiento de los registros puede llevarse a cabo de manera digital o manual.
En los casos en que el formato se diligencie de manera manual, se deben tener en cuenta los siguientes aspectos:

- Escribir con letra clara y legible
- Usar tinta indeleble
- Diligenciar todas las casillas que el formato solicita.
- Evitar tachones y enmendaduras.
- Cuando ocurra un error que requiera la anulación del documento debe tacharse con una sola línea diagonal y dejar constancia mediante la firma y fecha del funcionario responsable.
- Cuando una casilla del formato que requiera diligenciamiento, no se diligenció, debe trazarse una línea para evitar diligenciamientos posteriores de información.

5.2 Responsabilidad

Para identificar quién es el responsable de diligenciar el documento es necesario implementar la Línea de Responsabilidad que se encuentra al final de los formatos establecidos, dicha línea de responsabilidad contiene los siguientes datos, de acuerdo a la naturaleza de cada formato:

	DILIGENCIADO POR
NOMBRE	
CARGO	
FIRMA	
FECHA	

	DILIGENCIADO POR	APROBADO POR
NOMBRE		
CARGO		
FIRMA		
FECHA		

	DILIGENCIADO POR	REVISADO POR	APROBADO POR
NOMBRE			
CARGO			
FIRMA			
FECHA			

Los Registros se relacionan en un Listado Maestro de Registros, código SGSI-FR-16, formato en el que se registran los siguientes datos:
Código, Nombre, Versión, Vigencia, Fecha de Vigencia, Ubicación o Dependencia, Lugar de Almacenamiento, Cargo del Responsable del Manejo del Archivo, Medio de Almacenamiento, Nivel de Acceso de la Información, Tiempo de Retención, Disposición Final y Observaciones. El responsable del diligenciamiento del listado maestro de registros es el líder de cada proceso o su delegado, quien debe reportar dentro de los cinco (5) últimos días de cada mes a la Unidad de Archivo y Correspondencia los cambios realizados en el listado.

Central de Operaciones Policiales de la Región Policial Junín

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PLAN DEL PROYECTO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Versión: 01

Código	**:**	**CPPISGSI**
Fecha	**:**	**11/12/2016**
Creado por	**:**	**Jean Carlo Zacarias Villafranca**
Aprobado por	**:**	**Jefe de Estado Mayor-OFIPLAAD**
Nivel de Confidencialidad	**:**	**Intimo / Intermedio / Superficial**

CONTENIDO

PLAN DEL PROYECTO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del Plan del proyecto es definir claramente el propósito del proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), los documentos que se redactarán, los plazos, las funciones y responsables del proyecto.

El Plan del proyecto se aplica a todas las actividades realizadas en el proyecto de implementación del SGSI.

El Plan del proyecto se aplica en una primera etapa a los datos, sistemas de información, medios de enlace y redes de comunicación, infraestructura tecnológica, soportes de información, infraestructura física y funcionarios que apoyan la ejecución de los tres (3) primeros procesos identificados como críticos dentro de la Central de Operaciones Policiales de la Región Policial Junín, lo cual nos permitirá identificar la metodología de implementación adecuada, para cada año adaptar los demás procesos críticos del negocio con el SGSI, hasta obtener un grado de madurez que luego nos permita gestionar de una manera adecuada todos los procesos en la Central de Operaciones Policiales de la Región Policial Junín.

Los usuarios de este documento son los efectivos policiales de la Central de Operaciones Policiales de la Central de Operaciones Policiales de la Región Policial Junín y los miembros del equipo del proyecto. Para este caso el Sr. gral. Jesús Moisés Ríos Vivanco Jefe de la Región Policial Junín, crnl. PNP Manuel Tafur Torres Jefe del Estado Mayor de la Región Policial Junín, componen el comando institucional encargado de la Institución Policial en la Región Junín, los mismos que tomarán las decisiones; asimismo, el equipo del proyecto está conformado por Jean Carlo Zacarias Villafranca.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001
- Norma ISO 22301

3. PROYECTO DE IMPLEMENTACIÓN DEL SGSI

3.1 Objetivo del proyecto

La implementación del Sistema de Gestión de Seguridad de la Información de conformidad con la norma ISO 27001:2013, se realizará hasta finales del mes de diciembre del 2016, para obtener los documentos necesarios que permitan gestionar de manera segura el flujo de información derivado de los diferentes procesos de la institución policial.

3.2 Resultados del proyecto

Durante el proyecto de implementación del SGSI, se redactarán los siguientes documentos:

a. Situación actual
b. Políticas que incluyen controles para:
   1) Aspectos organizativos de la seguridad de la información.
   2) Gestión de activos.
   3) Seguridad relacionada al personal.
   4) Gestión de comunicaciones y operaciones.
   5) Control de acceso.
   6) Adquisición, desarrollo, mantenimiento de sistemas informáticos.
   7) Gestión de los incidentes de seguridad.
   8) Gestión de la continuidad del negocio.
   9) Cumplimiento.
c. Compromiso por parte de los miembros del Comando Institucional de la Región Policial Junín, quienes conformarán el Comité de Administración Integral de Riesgo (CAIR), para apoyar decididamente a la implementación del SGSI.
d. Enfoque de evaluación de riesgos cuya metodología debe contemplar inventario de activos, identificación de amenazas y vulnerabilidades, identificación de impactos, análisis y evaluación de riesgos y tratamiento de riesgos.
e. Declaración de aplicabilidad SOA.
f. Estrategias para formación y concientización.
g. Planes de acción correctiva/preventiva.
h. Planes de monitoreo y revisión.
i. Revisión del SGSI por parte de la Dirección.
j. Planes de auditoría.

3.3 Plazos

El Sistema de Gestión de Seguridad de la Información tiene como fecha límite para su desarrollo el mes de febrero del 2017, fecha en la cual se habrá pasado por las fases del ciclo de *Deaming* o PDCA (*Plan-Do-Check-Act*) que nos permitirá, como la mejor práctica, hacer una mejora continua de las fases que son necesarias a fin de llevar a cabo una satisfactoria implementación del SGSI.

3.4 Organización del proyecto

2.1 Promotor del proyecto

El promotor y responsable del presente proyecto será Jean Carlo Zacarias Villafranca, quien deberá coordinar cada una de las fases, solicitar, organizar o generar la documentación que sea necesaria a fin de dar cumplimiento a la implementación del SGSI.

2.2 Gerente del proyecto

El ss. PNP Huamán Pari Jefe de la Oficina de Planeamiento Administrativo del Estado Mayor de la Región Policial Junín, informará de los avances en el desarrollo del presente proyecto al Sr. gral. Jesús Moisés Ríos Vivanco Jefe de la Región Policial Junín.

2.3 Equipo del proyecto

Para el desarrollo del presente proyecto será necesario contar con la colaboración de un miembro de la Oficina de Planeamiento Administrativo del Estado Mayor de la Región Policial Junín, Administrador de la oficina de Tecnologías de la Información y Comunicación de la Región Policial Junín y el Visto Bueno del Jefe de la Central de Operaciones Policiales con la finalidad de involucrar a sus colaboradores de una manera planificada.

3.5 Principales riesgos del plan

En cualquier proyecto, el recurso más importante son las personas. Idealmente un proyecto debería tener disponibles a un número adecuado de personas, con las habilidades y experiencia correctas, comprometidos y motivados con el proyecto. Sin embargo, las cosas pueden ser diferentes, por lo que hemos identificado los siguientes riesgos:

- ¿El personal del proyecto está comprometido con la entera duración para lo que son necesarios?
- ¿Todos los miembros del equipo están disponibles a tiempo completo?
- ¿El movimiento de personal de un mismo proyecto es suficientemente bajo como para permitir la continuidad del proyecto?
- ¿Se han establecido los mecanismos apropiados para permitir la comunicación entre los miembros del equipo?
- ¿El entorno de trabajo del equipo es el apropiado?

3.6 Herramientas para Implementación del proyecto y generación de informes

Se han evaluado varias herramientas, una de las mejores opciones de código abierto ha sido *Securia* SGSI, que es una herramienta integral que cubre el proceso automático de implantación, puesta en funcionamiento, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma internacional ISO 27001, además el análisis de riesgo se realizara con la herramienta *Pilar*.

La herramienta seleccionada es actualizada periódicamente y cuenta con manuales de implementación y uso en español, adicionalmente se usarán hojas de cálculo lo cual permitirá llevar un control del avance de la implementación del SGSI.

4. GESTIÓN DE RIESGOS GUARDADOS EN BASE A ESTE DOCUMENTO

Se realizará una revisión de los documentos de políticas y archivos generados del desarrollo e implementación del SGSI, se gestionará la implementación de un sistema de versionamiento que permita validar los cambios documentales y las versiones finales donde adicionalmente se llevará el control de la documentación en las herramientas seleccionadas.

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS.

Todos los documentos serán debatidos por los involucrados, recoger los comentarios ayudará a enriquecer las políticas que se definan, solo entrará en vigencia cuando se los apruebe por los canales establecidos en la institución policial, y una vez que se tengan implementadas todas las correcciones solicitadas por los involucrados del SGSI.

6. DIAGNÓSTICO SITUACIÓN ACTUAL

6.1 Objetivos

- Verificar la implementación de una metodología que permita gestionar los riesgos de la Institución Policial, la identificación y valoración de activos y las amenazas sobre estos.
- Verificar la administración de accesos lógicos a los servicios internos y externos.
- Verificar las configuraciones de los servicios y la documentación generada.
- Evaluación de la arquitectura de red implementada.
- Seleccionar los controles que nos van a permitir cubrir los distintos aspectos al implementar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Revisar las políticas, normas, procedimientos y documentos de control que nos permiten determinar el grado de cumplimiento en la implementación del SGSI.

6.2 Metodología

La metodología seleccionada para la implementación se basa en la metodología EISA la cual nos permitirá aplicar un método riguroso y comprensivo para describir el comportamiento de los procesos de seguridad, sistemas de seguridad de información y subunidades policiales, para que se alineen con las metas comunes de la organización y la dirección estratégica.

Preguntas que responde la EISA:
Un proceso de Arquitectura de Seguridad de Información en la empresa ayuda a contestar preguntas básicas como:

- ¿Está la arquitectura actual apoyando y añadiendo valor a la seguridad de la organización?
- ¿Cómo podría una arquitectura de seguridad ser modificada para que añada más valor a la organización?

Para implementar una arquitectura de seguridad de información que se alinee con la estrategia de la organización y otros detalles necesarios tales como dónde y cómo opera, es necesario contar con competencias esenciales, procesos de negocio y cómo la organización interactúa consigo misma.

Cuadro N° 1: Requerimientos en la Central de Operaciones Policiales de la Región Policial Junín

REQUERIMIENTO	DOCUMENTADO	ACTUALIZADO
Cuadros de organización, actividades y flujo de procesos de las operaciones de TI	SÍ	NO
Ciclos, periodos y distribución en el tiempo de la organización	NO	NO
Proveedores de tecnología hardware, software y servicios	SÍ	NO
Inventarios y diagramas de aplicaciones y software	SÍ	NO
Interfaces entre aplicaciones; esto es: eventos, mensajes y flujo de datos	NO	NO
Intranet, Extranet, Internet, comercio electrónico	NO	NO
Clasificación de datos, bases de datos y modelos de datos soportados.	NO	NO
Hardware, plataformas, servidores, componentes de red y dispositivos de seguridad y dónde se conservan	NO	NO
Redes de área local y abiertas, diagramas de conectividad a Internet	NO	NO

Fuente: elaboración propia

Para el desarrollo del presente plan se utilizarán los siguientes procedimientos:

- Reuniones con los involucrados en el Plan de implementación del SGSI, que nos permitirá debatir y contar con la aceptación de los controles de la norma ISO 27002 a implementar en la Central de Operaciones Policiales de la Región Policial Junín.
- Reunión para establecer el compromiso y delegados en el proceso de implementación del SGSI.

El objetivo de esta etapa es sentar las bases del proceso de mejora continua en materia de seguridad, permitiendo a la Central de Operaciones Policiales de la Región Policial Junín, conocer el estado del mismo y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales.

Para ello se abordarán las siguientes fases:

- Documentación normativa sobre las mejores prácticas en seguridad de la información.

- Identificación y valoración de los activos y amenazas sobre los activos de la Central de Operaciones Policiales de la Región Policial Junín.
- Auditoría de cumplimiento de la ISO/IEC 27002:2008.
- Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- Presentación de resultados.

Para adaptar el Sistema de Gestión de Seguridad de la Información será importante que el proyecto se ajuste a las 4 fases definidas por la serie de normas ISO 27000 como la mejor práctica para poder implementar el SGSI, en el siguiente esquema se presentan las etapas, en las cuales el SGSI será adaptado a la Central de Operaciones Policiales de la Región Policial Junín, las mismas etapas serán la guía para la presentación de avances.

6.3 Documentación normativa sobre las mejores prácticas en seguridad de la información

Para la ejecución de la presente etapa se selecciona a ***Magerit* V3** como metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, también es posible que para la consecución de los objetivos sea necesario implementar otras fuentes de buenas prácticas como ITIL.

6.4 Identificación y valoración de los activos y amenazas sobre los activos de la institución policial

6.4.1 Inventario de activos

Como primera actividad a ejecutar es necesario realizar la evaluación de los activos de información en los procesos seleccionados, considerando las dependencias entre estos y realizando una valoración.

Cuadro N° 2: activos de la institución

INVENTARIO DE ACTIVOS	DETALLES
INSTALACIONES	Ubicación de equipos informáticos y de comunicaciones
HARDWARE (HW)	Equipos que alojan datos, aplicaciones y servicios
APLICACIONES (SW)	Aplicativos que permiten manejar los datos
DATOS	El principal recurso, todos los demás activos se identifican alrededor de éste activo
RED	Equipamiento que permite intercambiar datos

SERVICIOS	Que se brindan gracias a los datos y que se necesitan para gestionar los datos
EQUIPAMIENTO AUXILIAR	Todo aquello que complemente al material informático
SOPORTES DE INFORMACIÓN	Dispositivos que permiten el almacenamiento de datos (temporal)
PERSONAL	Quienes explotan u operan todos los demás elementos

Fuente: elaboración propia

Cuadro N° 3: dimensiones de seguridad

DIMENSIONES DE SEGURIDAD		
VA	**VALOR**	**CRITERIO**
MA	10	Daño muy grave a la organización
A	7-9	Daño grave a la organización
M	4-6	Daño importante a la organización
B	1-3	Daño menor a la organización
MB	0	Daño irrelevante para la organización

Fuente: *Magerit* V3

Cuadro N° 4: ámbito y activos

ÁMBITO	ACTIVO	VALOR
DATOS	Información personal	MA
	Imágenes digitales	MA
SERVICIO	Trámites policiales	M
	Consultas policiales	M
SW	CHASKA PI3	MA
	Telegram	MA
	Correo electrónico	MA
HW	Terminales de usuario	A
REDES Y COMUNICACIONES	Red LAN	A
SOPORTE DE INFORMACIÓN	Notas informativas	MA
	Notas de información	MA
INSTALACIONES	Oficinas	A
PERSONAL	Oficial de órdenes	MA
	Analistas de información	MA
	Personal técnico	MA

Fuente: elaboración propia

6.4.2 Análisis de amenazas

Para el entendimiento de la presente etapa es necesario indicar que se establecen según *Magerit* V3, ciertas amenazas típicas identificadas y que reducen la utilización del activo en diferentes ámbitos de los pilares de la seguridad de la información, estos

activos están frecuentemente expuestos a las amenazas, por lo cual la frecuencia de ocurrencia se expresará como tasa anual o incidencias por año; finalmente la frecuencia con la que una amenaza se materialice sobre un activo hará que este activo disminuya en un porcentaje de su valor.

6.4.3 Calculo del riesgo

El cálculo del riesgo actual es una valoración en la que interviene el valor que le hemos dado a los activos en cada una de las dimensiones, la frecuencia con la que una amenaza puede degradar a un activo y el impacto de daño o disminución que la amenaza puede causarle al activo.

6.4.4 Selección de controles - salvaguardas

Para ejecutar la actividad de selección de salvaguardas, debemos tomar en consideración los elementos de protección actual que tienen nuestros activos y los posibles elementos de control de los que podemos dotar a nuestros activos, es decir a los grupos de activos que hemos definido, validar los controles del Anexo a la Norma UNE-ISO/IEC 27001:2013 son aplicables en el contexto de nuestras capacidades, para esto se han considerado 2 ámbitos esenciales con los que debemos trabajar las salvaguardas, los aspectos y el tipo de protección de las salvaguardas que vamos a implementar, los cuales resumimos en los siguientes cuadros.

			TIPO DE PROTECCIÓN	
			PTG	Protección de tipo general
ASPECTOS DE LAS SALVAGUARDAS			PdS	Protección de servicios
			PDI	Protección de datos/información
PR	Procedimientos		PSW	Protección de aplicaciones
PP	Política personal		PHW	Protección de equipos
SW	Aplicaciones		PdC	Protección de comunicaciones
HW	Dispositivos físicos		PSF	Seguridad física
SF	Seguridad física		PRP	Relativas al personal

Fuente: *Magerit* V3

6.4.5 Auditoria de cumplimiento de la ISO 27001

Con el propósito de proteger la información de la institución policial, y como futura guía para implementar o mejorar las medidas de seguridad, esta etapa nos va a permitir obtener una

radiografía de la situación actual en torno a la seguridad de la comisaria.

Central de Operaciones Policiales de la Región Policial Junín

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE REQUERIMIENTOS

Versión: 01

Código	**:**	**CPIR**
Fecha	**:**	**16/12/2016**
Creado por	**:**	**Jean Carlo Zacarias Villafranca**
Aprobado por	**:**	**Jefe de Estado Mayor-OFIPLAAD**
Nivel de Confidencialidad	**:**	**Intimo / Intermedio / Superficial**

CONTENIDO

PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE REQUISITOS

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir el proceso de identificación de las partes interesadas, de los requisitos legales, normativos, contractuales y de otra índole relacionados con la seguridad de la información y con la continuidad del negocio, como también los responsables de su cumplimiento. Este documento se aplica a todo el Sistema de gestión de seguridad de la información (SGSI). Los usuarios de este documento son todo el personal policial de la Central de Operaciones Policiales de la Región Policial Junín.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, punto 4.2; control A.18.1.1
- Norma ISO 22301, punto 4.2
- Política del sistema de gestión de seguridad de la información
- Política de la Continuidad del Negocio

3. IDENTIFICACIÓN DE REQUISITOS Y PARTES INTERESADAS

El may. PNP Elmer Quintanilla Camargo Jefe de la Central de Operaciones Policiales de la Región Policial Junín, será el responsable de brindar toda la información requerida para la determinación y levantamiento de requisitos.

Requerimientos de la Central de Operaciones Policiales de la Región Policial Junín:

REQUERIMIENTO	DOCUMENTADO	ACTUALIZADO
Cuadros de organización, actividades y flujo de procesos de las operaciones de TI	SÍ	NO
Ciclos, periodos y distribución en el tiempo de la organización	NO	NO
Proveedores de tecnología hardware, software y servicios	SÍ	NO
Inventarios y diagramas de aplicaciones y software	SÍ	NO
Interfaces entre aplicaciones; esto es: eventos, mensajes y flujo de datos	NO	NO
Intranet, Extranet, Internet, comercio electrónico	NO	NO
Clasificación de datos, bases de datos y modelos de datos soportados	NO	NO
Hardware, plataformas, servidores, componentes de red y dispositivos de seguridad y dónde se conservan	NO	NO
Redes de área local y abiertas, diagramas de conectividad a Internet	NO	NO

Fuente: RP Junín-Ceopol

4. RESPONSABLES

Responsables de la información

R: Responsabilidad - C: Colaboración

	Jefe Ceopol	CTSG
Recopilación de legislación de seguridad		R
Identificación de requisitos legales de seguridad		R
Evaluación del riesgo de cumplimiento	C	R
Adopción de medidas para asegurar el cumplimiento		R
Actualización de lista de requisitos legales	C	R
Comunicación	R	C
Cumplimiento y archivos de registros		R

Fuente: RP Junín-Ceopol

Central de Operaciones Policiales de la Región Policial Junín

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Versión: 01

Código	**:**	**CASGSI**
Fecha	**:**	**19/12/2016**
Creado por	**:**	**Jean Carlo Zacarias Villafranca**
Aprobado por	**:**	**Jefe de Estado Mayor-OFIPLAAD**
Nivel de Confidencialidad	**:**	**Intimo / Intermedio / Superficial**

CONTENIDO

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo de este documento es definir claramente los límites del Sistema de Gestión de Seguridad de la Información (SGSI) de la Central de Operaciones Policiales de la Región Policial Junín.

Este documento se aplica a toda la documentación y actividades dentro del SGSI.

Los usuarios de este documento son los efectivos policiales de la Central de Operaciones Policiales de la Región Policial Junín.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, punto 4,3
- Plan del proyecto para la implementación de la norma ISO 27001
- Lista de requisitos legales, normativos, contractuales y de otra índole

3. DEFINICIÓN DEL ALCANCE DEL SGSI

La organización policial necesita definir los límites del SGSI para decidir qué información quiere proteger, dicha información deberá ser protegida independientemente de si además es almacenada, procesada o transferida dentro o fuera del alcance del SGSI. El hecho que determinada información esté disponible fuera del alcance no significa que no se le aplicarán las medidas de seguridad, esto implica que la responsabilidad por la aplicación y de las medidas de seguridad serán transferidas a un tercero que administre dicha información.

Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del SGSI se define de acuerdo a los siguientes aspectos:

3.1 Procesos y servicios

Dentro de los procesos que se dan en la Central de Operaciones Policiales de la Región Policial Junín, tenemos los siguientes:

- Mantener informado al Jefe de la Región Policial Junín del resultado de las operaciones policiales y hechos relevantes que se suscitan en las Divisiones que conforman esta Dirección Policial, utilizando la aplicación de escritorio *Telegram*, mediante comunicaciones telefónicas y documentos impresos.
- Recibir notas informativas e imágenes digitales vía correo electrónico sobre las operaciones policiales que se ejecutan en las Divisiones que conforman esta Dirección Policial (Provincias de Huancayo, Jauja, Concepción, Chupaca, Chanchamayo, Satipo, Tarma, Yauli La Oroya y Junín).
- Centralizar y procesar la información policial tanto operativa como administrativa para dar cuenta a la Superioridad.
- Procesa la documentación en general proveniente del comando institucional Dirgen, Dirnop (ahora Subdirgen) y otros, para su distribución a las diferentes unidades y subunidades.

- Remite vía correo electrónico diferentes documentos a la Dirgen, Mininter y a las Unidades y Subunidades PNP.
- Formular Notas Informativas y demás documentos que se tramitan de la Región Policial Junín a otras dependencias policiales, civiles y militares, así como a las Unidades y Subunidades de su ámbito de responsabilidad.
- Anota el ingreso y egreso de documentos en general en el cuaderno de registros.
- Transmite las Ordenes Telefónicas dispuesta por la Superioridad.
- Recibe información telefónica sobre cualquier hecho las 24 horas del día.
- Orienta a los SSOO. PNP de Órdenes y analistas de información para la captación de información complementaria que se requiere para su procesamiento respectivo.
- Imparte instrucción al personal de Oficiales y Suboficiales PNP a fin de que cumplan las funciones en forma eficaz, eficiente y oportuna.
- Realiza otras funciones que le asigne la Superioridad.

3.2 Unidades organizativas

La Central de Operaciones Policiales de la Región Policial Junín es un órgano de apoyo a la Jefatura de la Región Policial Junín.

Asimismo, se adscriben directamente a la Jefatura de la Región Policial Junín, los siguientes grupos:

a. Jefatura y Ceopol.
b. Secretaria.
c. OFAD-Recursos Humanos.
d. Estado Mayor-Oficina de Planeamiento Administrativo y de Instrucción

Los mencionados grupos tendrán carácter central.

Jefatura de la Región Policial Junín

1. Corresponde a la Dirección de la Región Policial Junín, por medio de la Oficina de Secretaría la realización de las tareas siguientes:
   - Recepción, registro y distribución de toda la documentación de la institución policial.
   - Gestión de la comunicación interna y externa de la institución policial en coordinación con las unidades competentes en materia de la administración.
   - Atención de las relaciones institucionales con otras unidades y subunidades PNP, por medio de la Oficima y Ofiparci.
   - Recopilación y divulgación de normativa y procedimientos aplicables a la operatividad policial.
   - La elaboración de informes jurídicos y asesoramiento por medio de Asesoría Legal.
   - Centralización y apoyo a las áreas y comisarías de todas las tareas generales de carácter administrativo.

- Gestión y control de la documentación de la institución policial inspeccionando su correcta tramitación en los plazos establecidos, así como su registro, archivo y custodia.
- Identificación y atención de las necesidades de la institución Policial en Recursos Humanos en coordinación con la Dirección Ejecutiva de Personal de la PNP.
- Gestión y tramitación de todo lo relacionado con licencias, permisos, vacaciones, situaciones administrativas, control de horarios, provisión de puestos de trabajo, así como velar por el cumplimiento de las disposiciones vigentes, por medio de la Ofirehum.
- Gestión y control de los expedientes personales de los componentes de la institución.
- Desarrollo de una cultura preventiva de riesgos laborales, impulsando acciones oportunas de acuerdo a la legislación específica, la elaboración de los planes de prevención de riesgos laborales y coordinación con las unidades competentes de la administración.
- Gestión económica y presupuestaria de la institución policial en coordinación con las Unidades Ejecutoras de la institución policial, por medio de la OFAD.
- Gestión de los ingresos recaudados por concepto de elaboración de informes policiales, tasas, antecedentes policiales y servicios especiales, por medio de la OFAD.
- Revista de armas en colaboración con la División de Armamento.

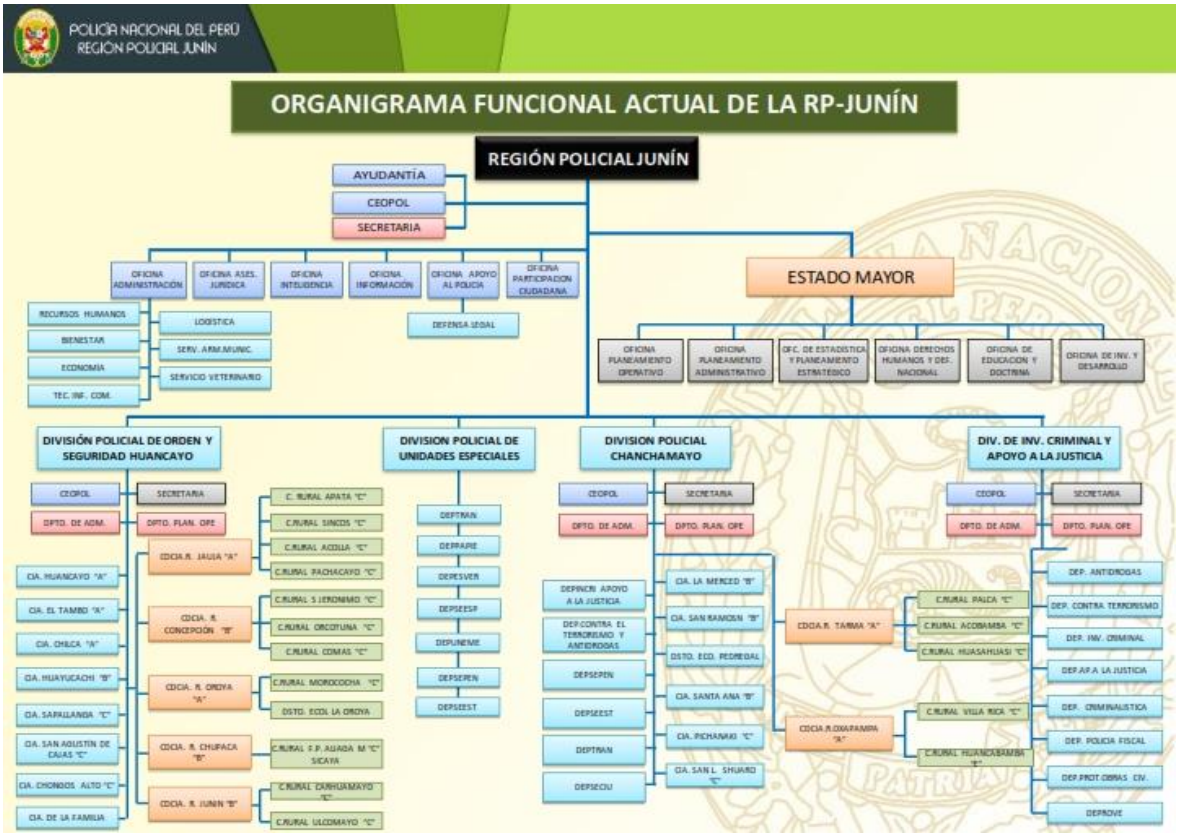


Figura A. Organigrama de la Región Policial Junín

Fuente: Regpol Junín-Estado Mayor/Ofiplaad

3.3 Redes e infraestructura de TI

Cuadro N° 1: Infraestructura de TI de la institución

GRUPO	TIPO	DESCRIPCIÓN	UNIDADES
Hardware	Equipos de cómputo - oficina	PCs de escritorio	14
		Celulares	03
	Impresoras	Impresora matricial B/N	04
		Impresora multifuncional escáner oficina	06
	Dispositivos de red	*Switches* C3 distribución oficinas	04
		Switches C3 distribución CPD	02
		Routers CPD	02

Fuente: RP Junín/Ceopol

Cuadro N° 2: infraestructura de TI de la institución

GRUPO	TIPO	DESCRIPCIÓN	UNIDADES
Infraestructura	CPD	Generador eléctrico	01
		Radio de comunicaciones	01
		Armarios de comunicaciones	01
		Armarios	04

Fuente: RP Junín/Ceopol

Central de Operaciones Policiales de la Región Policial Junín

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Versión: 01

Código	**:**	**CPSI**
Fecha	**:**	**27/12/2016**
Creado por	**:**	**Jean Carlo Zacarias Villafranca**
Aprobado por	**:**	**Jefe de Estado Mayor-OFIPLAAD**
Nivel de Confidencialidad	**:**	**Intimo / Intermedio / Superficial**

CONTENIDO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CENTRAL DE OPERACIONES POLICIALES DE LA REGIÓN POLICIAL JUNÍN

1. OBJETIVO, ALCANCE Y USUARIOS

La presente política de alto nivel tiene como propósito definir el objetivo, dirección, principios, disposiciones y reglas básicas para la gestión de la seguridad de la información en la Central de Operaciones Policiales de la Región Policial Junín.

Además, esta política está dirigida a todos los efectivos policiales operadores de información y usuarios de los sistemas de información de la Central de Operaciones Policiales de la Región Policial Junín.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales (MOF CEOPOL).
- Ley N° 29733 Ley de protección de datos personales 03JUL11.
- Régimen Disciplinario de la Policía Nacional del Perú D.L. N° 1268 del 16DIC16.
- Manual de documentación policial 2016 R.D. N° 776-2016-Dirgen/EMG-PNP del 27JUL16.

3. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN

- **Confidencialidad**: característica de la información que está disponible solo para personas o sistemas autorizados.
- **Integridad**: característica de la información que es modificada solo por personas o sistemas autorizados y de una forma permitida.
- **Disponibilidad**: característica de la información a la cual pueden acceder solo las personas autorizadas cuando sea necesario.
- **Seguridad de la información**: es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de gestión de seguridad de la información**: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. OBJETIVOS DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1. Objetivo general

Lograr niveles aceptables de integridad, confidencialidad y disponibilidad de la información policial, con el objeto de asegurar continuidad operacional de los procesos que desarrolla la Central de Operaciones Policiales de la Región Policial Junín, mediante el resguardo de los activos de información asociados a los procesos críticos del negocio y su soporte.

4.2. Objetivos específicos

- Identificar, clasificar y asignar los activos de información de la institución policial, para lograr niveles adecuados de integridad, confidencialidad y disponibilidad de la información.
- Controlar, prevenir y/o mitigar los riesgos de seguridad de la información, identificando las vulnerabilidades y amenazas que enfrentan los activos, para asegurar la continuidad del negocio.
- Establecer políticas, normativas y procedimientos que permitan resguardar y proteger los activos de información de la institución policial.
- Definir un Plan de Instrucción y Capacitación que permita difundir los alcances y buenas prácticas asociadas a la seguridad de la información institucional.

5. ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

5.1. Alcance general

La Política General de Seguridad de la Información de la Central de Operaciones Policiales de la Región Policial Junín, se establece en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información.

La presente política debe ser conocida y cumplida por todo el personal de la Central de Operaciones Policiales de la Región Policial Junín involucrada en el uso de los sistemas y tecnologías de Información y las notas informativas.

Esta política se aplica en todo el ámbito de la institución policial a nivel Región Policial Junín, a sus recursos y a la totalidad de los procesos, internos y externos.

De lo anterior, la información que genera y gestiona la institución policial constituye un activo estratégico clave para asegurar la continuidad del negocio; por lo que, la Seguridad de la Información es una herramienta para garantizar su integridad, disponibilidad y confidencialidad.

5.2. Definición de los activos de información

Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución policial, en la que se distinguen tres niveles:

- La información propiamente dicha, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- Los equipos, sistemas e infraestructura que soportan la información.
- El personal policial que utiliza la información y que tienen conocimiento de los procesos institucionales.

ACTIVOS DE INFORMACIÓN

ACTIVOS DE INFORMACIÓN	ACTIVOS FÍSICOS	ACTIVOS DE SERVICIOS DE TI	ACTIVOS HUMANOS
Notas informativas formato digital y físico	Infraestructura de TI	Servicios de autenticación	Personal policial de la CEOPOL y OFINTE
Datos digitales en BBDD PI3	Oficinas y muebles	Servicios de red, conectividad, red LAN	
Imágenes digitales	Ordenadores y equipos informáticos (HW)		
Correo electrónico comercial/doméstico y app *Telegram Desktop*	Instalaciones		

Fuente: elaboración propia

CAPITAL HUMANO
ESTRUCTURACIÓN Y VALOR DE LOS ACTIVOS

GRUPO	DESCRIPCIÓN	UNID.	VALOR	CRITICIDAD
Personal policial	Operadores	30	Muy alta	Alta
	Jefes	02	Muy alta	Alta

Fuente: elaboración propia

DESCRIPCIÓN Y VALOR CRÍTICO DE LOS ACTIVOS

TIPO	DESCRIPCIÓN	UNID	VALOR	CRITICIDAD
Equipos de oficina	Equipos de cómputo	25	Media	Media
	Impresoras	6	Baja	Baja

Fuente: elaboración propia

5.3. Definición de la seguridad de la información

La Central de Operaciones Policiales de la Región Policial Junín, entiende que la seguridad de la información es la protección de los activos de información contra una amplia gama de amenazas y vulnerabilidades; por lo que, se debe asegurar la continuidad de las operaciones, minimizar el daño a la institución y maximizar la eficiencia y las oportunidades de mejora de la gestión.

6. Políticas y objetivos de seguridad de la información

Las políticas de seguridad que se plantean en este documento, están basadas en un análisis estratégico acorde con cada una de las fases de la estrategia, misión y visión de la organización.

Estas políticas representan directrices generales de alto nivel que deben ser adoptadas por los integrantes en la cadena de prestación de servicios durante las fases de la evolución de la estrategia de la institución policial. Para asegurar el cumplimiento de las políticas de seguridad para la institución, se establecieron objetivos de control asociados a cada política:

6.1. Política de control de acceso

Del análisis y evaluación de riesgos se determinó que se requiere mayor nivel de seguridad; por lo que, se debe implementar mecanismos y controles que aseguren un registro efectivo, identificación y autenticación de los usuarios de dichos servicios como PI3-CHASKA. Asimismo, se debe implementar mecanismos y controles que aseguren el acceso bajo el principio del menor privilegio, necesario para realizar únicamente las labores de cada usuario de dicho servicio.

Objetivos control

PS1.1	Otorgar acceso al sistema web PI3-CHASKA solo a usuarios autorizados. Se requiere limitar el acceso solo para usuarios identificados y autenticados apropiadamente que presten servicios en la Ceopol y Ofinte.
PS1.2	Otorgar privilegios de acceso a servicios que requieren mayor nivel de seguridad en el uso del sistema web PI3-CHASKA. Se requiere minimizar el daño potencial causado por usuarios autorizados lo cual implica establecer segregación de funciones para separar usuarios de los servicios y usuarios con roles administrativos.
PS1.3	Otorgar acceso a servicios que requieren mayor nivel de seguridad condicionado a la presentación de información que soporte la identidad del individuo que requiere el acceso y sus credenciales de autenticación.
PS1.4	Otorgar privilegios de acceso a servicios de la institución, sólo cuando se satisfaga la verdadera identidad del usuario, es decir, que el usuario sea quien realmente dice ser y que no esté registrado bajo otra identidad con un acceso legítimo. Se debe evitar y prevenir la creación de usuarios múltiples. Un usuario puede tener múltiples roles con respecto a los servicios de la institución, pero solo puede poseer una única identidad.
PS1.5	Otorgar acceso a los usuarios sobre los servicios y activos necesarios para soportar el servicio específico requerido. No se deben alterar datos.

PS1.6	Implementar una administración efectiva de los derechos de acceso de usuarios y asignar dicha responsabilidad al personal apropiado, ello en coordinación con personal de administradores de accesos.
PS1.7	Implementar la vigencia de los derechos de acceso y su revocación, una vez finalice el período asignado o haya pérdida de las credenciales, o se detecte uso indebido de los recursos por parte de los usuarios. Las credenciales de acceso deben quedar inválidos ante eventos de revocación o cambio de colocación a otra subunidad.

6.2. Política de no repudio

Se debe garantizar el no repudio de las transacciones en los sistemas informáticos y aplicaciones web poniendo en práctica mecanismos de seguridad que permitan crear un ambiente de confianza entre el Sr. gral. Jefe de la Región Policial Junín y personal operador de la Ceopol, con relación a la autenticidad, trazabilidad y no repudio de las transacciones electrónicas.

Objetivos control.

PS2.1	Proveer evidencia del origen y la integridad del mensaje, es decir, se deben crear mecanismos en el servicio para crear una prueba de origen de la información de manera que se pueda evitar que una de las partes (Ceopol, comisaría o subunidad especializada) niegue su responsabilidad en el envío del mensaje ya sea por correo electrónico o vía sistema web PI3-CHASKA; por lo que se debe guardar la nota informativa de origen en formato digital e impreso. Asimismo, se deben implementar mecanismos para probar si el mensaje ha sido alterado.
PS2.2	Proveer evidencia del acuse del mensaje, es decir, se deben implementar mecanismos en el servicio de correo, como respuesta automática para crear una prueba de recibo, acuse recibo y almacenarla para su recuperación posterior, en caso de controversia entre las partes (Ceopol, comisaría o subunidad especializada), de igual manera se trabajará con el sistema web PI3-CHASKA, verificando su síntesis diaria.
PS2.3	Proveer evidencia que el servicio es proporcionado realmente por una entidad pública con relación al sistema web PI3-CHASKA. Se deben implementar credenciales del servicio, registrar correos oficiales, teléfonos de soporte y ser presentadas a los operadores para la autenticación del sistema web PI3-CHASKA.
PS2.4	Proveer evidencia de la fecha y hora de la transacción electrónica efectuada a través del servicio de correo y sistema web PI3-CHASKA.

6.3. Política de privacidad y confidencialidad

Los datos personales, imágenes digitales e impresas de detenidos, intervenidos y demás información enviada a través de los servicios de la institución policial, deben ser protegidos y manejados de manera responsable y segura.

Objetivos de control:

PS3.1	Proveer protección adecuada de la información personal y privada contra divulgación no autorizada cuando se transmite a través de redes vulnerables, llámese sistema web PI3-CHASKA, correo electrónico y app *Telegram*.
PS3.2	Normar y autorizar los destinatarios de los mensajes de correo que se remiten desde las comisarías y subunidades especializadas; asimismo, normar y filtrar periódicamente a los usuarios autorizados a la visualización de la información que se propala en el Grupo Comando de la Región Policial Junín por la app *Telegram*.
PS3.3	Proteger la información personal y privada de uso indebido y divulgación no autorizada en medios de fuente abierta, así como las imágenes de detenidos o intervenidos cuando se procesa y almacena dentro del dominio de implementación de los servicios de la institución policial y Ceopol.

6.4. Política de integridad

La información que se recibe o se envía a través de los servicios de la institución policial, debe conservar los atributos de correcta y completa durante la transmisión, el procesamiento y el almacenamiento. Deben garantizar la integridad de la información.

Objetivos de control:

PS4.1	Proteger la información que se transmite a través de redes públicas contra modificación, borrado o repetición accidental o intencional. Se debe asegurar la fuerte integridad de las comunicaciones para prevenir contra manipulación de datos en tránsito o contra fuga, pérdida y corrupción causada por fallas de equipos, comunicaciones y otros.
PS4.2	Proteger la información que se almacena contra modificación accidental o intencional. Se deben implementar mecanismos para prevenir que los operadores manipulen la información del servicio almacenada en su estación de trabajo con el fin de obtener algún beneficio.
PS4.3	Proteger la información almacenada dentro de los servicios de la institución policial (correo electrónico, app *Telegram* y sistema web PI3-CHASKA) contra modificación o destrucción intencional por parte de atacantes externos. Se deben implementar fuertes medidas para frustrar la alteración mal intencionada de los datos de usuarios o de

	información de dominio público que puedan disminuir la confianza de los servicios. Los proveedores de servicios tienen la obligación del debido cuidado, para asegurar que la información proporcionada sea veraz.
PS4.4	Proteger la información trasmitida o almacenada dentro de la institución policial contra pérdida o corrupción accidental. Se deben implementar procedimientos probados de respaldo y recuperación de datos y asegurar que se mantienen las listas de usuarios autorizados, dando cuenta a inspectoría en caso de modificación no comunicada.

6.5. Política de disponibilidad del servicio

Es de preponderante importancia poder asegurar la disponibilidad continua de los servicios bajo un control estricto y adecuado.

Objetivos de control:

PS5.1	Proteger los servicios de la institución policial contra daños, intrusión o negación por parte de atacantes externos, implementar un plan de contingencia ante este tipo de eventos.
PS5.2	Proteger los servicios de la institución policial contra daños o provisión intermitente del servicio por fallas internas de los equipos y/o redes. Se deben implementar mecanismos de redundancia y alta disponibilidad acordes con la criticidad de la provisión continua del servicio y la capacidad para realizar reparaciones rápidas.
PS5.3	Proteger los servicios de la institución policial contra pérdida de datos, pérdida de equipos y otros eventos adversos. Se debe implementar un plan de continuidad del Negocio (BCP-*Business Continuity Plan*), para asegurar que se toman las medidas necesarias y evitar en lo posible, la pérdida de información por ocurrencia de incidentes.

6.6. Política de disponibilidad de información

Las entidades de Gobierno deben asegurar que los datos de los usuarios y clientes se mantienen protegidos contra pérdida, alteración o divulgación por actos accidentales o malintencionados, o por fallas de los equipos y/o redes.

Objetivos de control:

PS6.1	Recuperar los datos personales o críticos que han sido dañados, destruidos, alterados o modificados por acciones malintencionadas o accidentales. Se deben implementar procedimientos de copias de respaldo y recuperación, archivos digitales de notas informativas, para asegurar que exista recuperación de los datos sensibles y que puedan ser restaurados en el evento de una falla. También se deben implementar mecanismos para que los datos personales no sean divulgados sin autorización expresa del propietario de la información, que viene a ser la Policía Nacional del Perú.

PS6.2	Recuperar la información protegida en el evento en el que un usuario no pueda suministrar las credenciales de acceso necesarias en el caso del uso del CHASKA-PI3. Se deben implementar procedimientos para recuperar datos de usuario en el evento que la contraseña se pierda. Esto permite soportar investigaciones de posible uso indebido del sistema.

6.7. Política de protección del servicio

Se debe asegurar que los servicios y sus activos de información relacionados, estén adecuadamente protegidos contra ataques externos o internos.

Objetivo de control:

PS7.1	Proteger los sistemas de información, equipos y redes que soportan los servicios de la institución policial contra ataques a la provisión continua y segura del servicio. Se deben asegurar los equipos y las redes implementando medidas como aseguramiento de servidores, implementación de topologías seguras de red y escaneo de vulnerabilidades. Los sistemas de información y las aplicaciones, deben ser diseñados e implementados de manera que se minimicen las vulnerabilidades y los ataques externos e internos se reduzcan a un nivel despreciable.

6.8. Política de registro y auditoria

Es importante el poder mantener y proteger los registros de las transacciones electrónicas como evidencia para los requerimientos de las auditorias (internas) y como mecanismo para establecer responsabilidades de los usuarios ante incidencias.

Objetivo de control:

PS8.1	Mantener un registro de transacciones que pueda ser requerido después del análisis de eventos y/o incidentes. Se deben mantener registros y pistas de auditoría con el fin de establecer responsabilidad por las transacciones, reconstruir transacciones fallidas y suministrar registros apropiados en caso de conflictos o disputas por el servicio. Debe existir trazabilidad de los registros de transacciones según sea apropiado.

6.9. Política de protección de los bienes jurídicos de la Policía Nacional del Perú

Es necesario privilegiar y salvaguardar los bienes jurídicos de la Policía Nacional del Perú, constituidos por la Ética Policial, la Disciplina Policial, el Servicio Policial y la Imagen Institucional, como bienes jurídicos imprescindibles para el cumplimiento adecuado de la función policial y el desarrollo institucional; por lo que, se enmarca en el D.L. N° 1268 del

16DIC16, que regula el Régimen Disciplinario de la Policía Nacional del Perú.

Objetivo de control:

PS9.1	No se debe ocultar, omitir o alterar información necesaria en documentos relacionados con el desempeño de la función policial que cause perjuicios.
PS9.2	No se debe promover o solicitar la difusión de hechos policiales con fines de protagonismo personal.
PS9.3	No emitir opinión sobre asuntos relacionados a la PNP haciendo uso de los medios de comunicación social, sin autorización del Comando.
PS9.4	No se debe promover o solicitar la difusión de hechos policiales con fines de protagonismo personal.
PS9.5	No entregar o divulgar información clasificada sin las formalidades legales, incluyendo la relacionada con la salud del personal de la Policía Nacional del Perú y sus familiares.
PS9.6	No utilizar o manipular medios técnicos o informáticos, imágenes o sonidos de propiedad o uso de la Policía Nacional del Perú en beneficio propio o de terceros.
PS9.7	Formular declaración o comentario no autorizado en forma pública sobre asuntos, que afecten la imagen y prestigio institucional.
PS9.8	Sustraer medios técnicos o informáticos, imágenes o sonidos de propiedad o uso de la Policía Nacional del Perú para fines distintos a los previstos legalmente, en beneficio propio o de terceros.
PS9.9	Omitir, borrar, agregar o alterar el registro de información oficial en las bases de datos informáticos de la Policía Nacional del Perú.
PS9.10	Difundir por cualquier medio, imágenes, documentos u otros relacionados con el servicio o el personal de la Policía Nacional del Perú, afectando la imagen institucional.

7. Marco general de las Políticas de Seguridad Institucional

7.1. Aspectos generales

La Política General de Seguridad de la Información ha sido elaborada en concordancia con la legislación policial vigente (Ley de Régimen Disciplinario PNP), considerando además su compatibilidad con las prácticas sugeridas por la Norma ISO/IEC 27001.

La Jefatura de la Región Policial Junín se compromete a realizar las acciones que estén a su alcance para permitir la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

7.2. Aprobación de la política

Las políticas de seguridad de la información serán aprobadas por el Sr. gral. PNP Jefe de la Región Policial Junín y Sr. crnl. PNP Jefe del Estado Mayor de la Región Policial Junín, reflejando claramente su compromiso, apoyo e interés en el desarrollo de una cultura de seguridad de la información en la institución policial.

7.3. Difusión de la política

Será responsabilidad del Jefe de la Central de Operaciones Policiales difundir los temas relevantes en materia de seguridad. Las políticas de seguridad de la información serán comunicadas a todo el personal y efectivos policiales.

Para la difusión de los contenidos de las políticas de seguridad de la información en el interior de la institución se deberán utilizar los medios de difusión que disponga el Sr. gral. PNP Jefe de la Región Policial Junín (correo electrónico, boletín digital informativo, etc.), así como también la Oficina de Instrucción del Estado Mayor de la Región Policial Junín.

Los principales medios utilizados serán:

- Boletín digital informativo de la institución.
- Manual de concientización.
- Inducción a personal que cubre servicios en la Ceopol y Ofinte cuando ingresen al servicio.
- Comunicaciones a través de charlas personalizadas y reuniones
- Se deberá definir, implementar y evaluar las acciones e iniciativas contenidas en un Plan de Difusión, Sensibilización, Instrucción y Capacitación en materia de seguridad de la información.

7.4. Revisión de la política

La Política General de Seguridad de la Información será revisada de manera anual o en las siguientes circunstancias:

- A requerimiento del Sr. gral. Jefe de la Región Policial Junín, frente a cambios en el ambiente de la institución, debido a las circunstancias del servicio, cambios generales, a las condiciones legales y al ambiente técnico.
- La modificación del presente documento está a cargo del Comité de Seguridad de la Información y será aprobado por el Sr. gral. Jefe de la Región Policial Junín.

7.5. Evaluación del cumplimiento de la política

Los Jefes de la Ceopol y Ofinte son responsables de la implementación de estas políticas de seguridad de la información, dentro de sus áreas de responsabilidad, así como el cumplimiento de las políticas, normativas y procedimientos por parte de su equipo de trabajo.

La institución realizará auditorías internas anuales al sistema de seguridad de la información para verificar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

El incumplimiento de la Política General de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características de las omisiones, dando cuenta documentadamente al órgano de control institucional.

7.6. Análisis diferencial de la institución policial

POLÍTICA DE SEGURIDAD				
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN				
Documento de política de seguridad de la información	SEGURIDAD	Existen normas que hacen referencia en cuanto al uso de los recursos informáticos e información de la institución.	No existe	No se cumple
Revisión de la política de seguridad	SEGURIDAD	Existen Políticas de Seguridad, aprobadas por la Dirección General o Dirección Ejecutiva de Información y Tecnologías de la Comunicación.	No existe	No se cumple
Procedimientos de seguridad de la información	SEGURIDAD	Existen procedimientos relativos a la seguridad de los Sistemas de Información	No existe	No se cumple
Responsable de las políticas, normas y procedimientos en Seguridad de la información	SEGURIDAD	Existe un responsable de las políticas, normas y procedimientos en Seguridad Informática	No existe	No se cumple
Comunicación de las normas	SEGURIDAD	Existen mecanismos para la comunicación a los usuarios de las normas	No existe	No se cumple
Verificar efectividad de las políticas	SEGURIDAD	Existen controles regulares para verificar la efectividad de las políticas	No existe	No se cumple

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD				
ORGANIZACIÓN INTERNA				
Compromiso de la jefatura en temas de seguridad con la información	SEGURIDAD	Existe un comité de gestión de la seguridad de la información y se ha realizado una asignación adecuada y definida de responsabilidades.	No existe	No se cumple
Evaluación de la adquisición y cambios de los Sistemas de Información	SEGURIDAD	Existe un responsable encargado de evaluar la adquisición y cambios de los Sistemas de Información	No existe	No se cumple
Coordinación en temas de seguridad dentro de la institución	SEGURIDAD	Existe coordinación entre los diferentes roles y funciones.	No existe	No se cumple
Responsables en temas de seguridad de información en la institución	SEGURIDAD	Están definidos los activos de información y aunque en algunos casos existe alguna asignación de responsabilidades, esta no se da de manera formal.	No existe	No se cumple
Acuerdo de confidencialidad	SEGURIDAD	Existe un acuerdo de confidencialidad de la información a la que se accede, se cree que es aceptable compartir información textual o imágenes sobre operaciones policiales de carácter confidencial sabiendo que se trata de un hecho de fuga de información y puede constituirse en delito de infidencia.	Existe	No se cumple

Niveles y acuerdos en temas de confidencialidad	SEGURIDAD	En algunos casos dentro de la institución se han realizado algunos acuerdos en temas de confidencialidad, pero muchas veces estos no se monitorean de manera periódica, mucho menos cuando se incorporan nuevos activos de información en la institución policial.	Existe	No se cumple
Autorización de recursos asociados a la seguridad de la información	SEGURIDAD	Existe un proceso de autorización para los nuevos recursos orientados a procesos de información, pero este proceso no es del todo formal, ya que no existe una documentación correspondiente.	Iniciado	No se cumple
Relación con otras subunidades	SEGURIDAD	Existen algunos procedimientos referenciados a prevenir algunos riesgos, pero en el caso de la seguridad de la información no se establece un procedimiento formal adecuado.	Iniciado	Cumple
Revisión independiente del referente a la seguridad de la información	SEGURIDAD	No específicamente en todas las áreas de la institución se realizan revisiones orientadas a temas de seguridad, ya que no cuentan con una política clara específica que termine definiendo la frecuencia y la metodología de la revisión.	No existe	No se cumple

GESTIÓN DE ACTIVOS				
RESPONSABLES DE LOS ACTIVOS EN LA INSTITUCIÓN				
Inventario de activos	SISTEMAS / REDES	El inventario de activos que son propiedad de la institución policial es adecuado.	Gestionado	No se cumple
Propietario de los activos	SISTEMAS / REDES	Al no existir un inventario, es asignado un propietario al activo de forma genérica y no específica.	Gestionado	No se cumple
Clasificación por criticidad	SISTEMAS / REDES	Se dispone de una clasificación de la información según la criticidad de la misma	Gestionado	No se cumple
Soporte a los activos de información	SISTEMAS / REDES	Están actualizados los sistemas operativos, antivirus, aplicaciones y programas de los equipos de cómputo; asimismo, estos son los adecuados.	Gestionado	Cumple
Controles y autenticación	SISTEMAS / REDES	Existe algún control en las redes para compartir archivos digitales	Gestionado	Cumple
Controles y autenticación	SEGURIDAD FÍSICA	Están configuradas pantallas de bloqueo en los equipos de cómputo dado el tiempo de inactividad	Gestionado	Cumple
Perímetro de seguridad	SEGURIDAD FÍSICA	El perímetro de seguridad física es eficiente (una pared, puerta con llave, control de acceso físico)	Gestionado	No se cumple
Registro de incidentes	RR.HH.	Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	Gestionado	No se cumple
Uso aceptable de los recursos informáticos en	RR.HH.	En la institución existe una publicación orientada a términos	Gestionado	No se cumple

la institución		de conducta y guía generalizada sobre el buen uso adecuado de los recursos de información.		
CLASIFICACIÓN DE LA INFORMACIÓN				
INFORMACIÓN DE LA INSTITUCIÓN				
Directrices de clasificación	RR.HH.	Se cuenta con una clasificación de información del personal efectivo de la institución, clasificando los activos de información que no contengan datos personales y tampoco se identifican según su criticidad para la institución.	Gestionado	No se cumple
Etiquetado y tratamiento en temas de seguridad	SEGURIDAD FÍSICA	La información clasificada suele estar etiquetada y tiene un tratamiento adecuado a las características, aunque con algunas limitaciones ya que a veces no está correctamente clasificada.	Gestionado	No se cumple
CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD				
POLÍTICAS DE SEGURIDAD				
Cumplimiento de las políticas y normas de seguridad	CUMPLIMIENTO	Ausencia de informes formales sobre revisiones del cumplimiento por parte de la jefatura, aunque en algunos casos de manera informal se suele realizar este seguimiento.	Gestionado	Cumple
Comprobación del	CUMPLIMIENTO	Se han realizados algunas auditorías	Gestionado	No se cumple

cumplimiento técnico		técnicas y procedimentales, la institución posee los informes, se analizan los resultados e informes y se implementan los resultados para beneficio de la institución.		
Informe o develación de incidentes	CUMPLIMIENTO	Existe un procedimiento formal de respuesta y se tiene en cuenta el cumplimiento de la legislación policial	Gestionado	No se cumple

Fuente: elaboración propia

RESUMEN DE ANÁLISIS DIFERENCIAL

DOMINIO	CUMPLE	NO CUMPLE
Política de seguridad	5%	95%
Organización de la seguridad y la información	40%	60%
Gestión de activos	60%	40%
Seguridad ligada a los RR.HH	25%	75%
Seguridad física y ambiental	55%	45%
Gestión de las comunicaciones y operaciones	35%	65%
Control de acceso	95%	5%
Adquisición, desarrollo y mantenimiento de sistemas de información	15%	85%
Gestión de incidencias de la seguridad de la información	5%	95%
Cumplimiento	30%	70%

Fuente: elaboración propia

GLOSARIO DE TÉRMINOS:

- **Evaluación de riesgos**
  Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del organismo.

- **Administración de riesgos**
  Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

- **Comité de Seguridad de la Información**
  El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas de la institución policial, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

- **Responsable de Seguridad Informática**
  Es la persona que cumple la función de supervisar el cumplimiento de la presente política y de asesorar en materia de seguridad de la información a los integrantes del organismo que así lo requieran.

- **Incidente de seguridad**
  Un incidente de seguridad es un evento adverso en un sistema de computadoras, aplicación informática o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Central de Operaciones Policiales de la Región Policial Junín

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN DE APLICABILIDAD

Versión: 01

Código	**:**	**CDA**
Fecha	**:**	**09/01/2017**
Creado por	**:**	**Jean Carlo Zacarias Villafranca**
Aprobado por	**:**	**Jefe de Estado Mayor-OFIPLAAD**
Nivel de Confidencialidad	**:**	**Intimo / Intermedio / Superficial**

CONTENIDO

DECLARACIÓN DE APLICABILIDAD

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir los controles adecuados a implementarse en la Central de Operaciones Policiales de la Región Policial Junín, además de identificar los objetivos, forma de implementación, aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.

Este documento incluye todos los controles detallados en el Anexo A de la Norma ISO/IEC 27001. Los controles se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI).

Los usuarios de este documento son el personal policial de la Central de Operaciones Policiales de la Región Policial Junín que se encuentran inmersos en las funciones del SGSI.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos 5.1.3 d)
- Política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Informe de evaluación y tratamientos de riesgos

3. APLICABILIDAD DE LOS CONTROLES

Son aplicables los siguientes controles del Anexo A de la norma ISO/IEC 27001:2013

ID	Controles norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Objetivos de Control	Método de implementación	Estado
A.5	Políticas de la seguridad de la información	SÍ	Políticas de seguridad de la información	La Dirección de la institución dará apoyo a la seguridad de la información, de acuerdo con los requisitos del negocio y las normas aplicables.	Planificado
A.5.1	Dirección de la gerencia para la seguridad de la información	SÍ	Documento de política de seguridad de la información	La dirección deberá aprobar un documento de políticas de seguridad de la información,	Planificado

				publicarlo y distribuirlo a todo el personal de la Ceopol	
A.5.1.1	Políticas para seguridad de la información	SÍ	Políticas de seguridad de la información	La dirección de la institución dará apoyo a la seguridad de la información, de acuerdo con los requisitos del negocio y las normas aplicables. Todas las políticas indicadas bajo esta columna	Planificado
A.5.1.2	Revisión de políticas para seguridad de la información.	SÍ	Revisión de políticas para seguridad de la información.	Cada política tiene un propietario designado que deberá revisar el documento según un intervalo planificado.	Planificado
A.6	Organización de la seguridad de la información	SÍ	Organización Interna	Gestionar la seguridad de la información dentro de la institución, mediante cargos y jerarquías	Planificado
A.6.1	Organización interna	SÍ	Organización Interna	Gestionar la seguridad de la información dentro de la institución, mediante cargos y jerarquías	Planificado
A.6.1.1	Roles y responsabili-dades sobre seguridad de la información	SÍ	Responsabilidades sobre los Activos de información	Asegurar el funcionamiento correcto y seguro de los recursos de tratamiento de la información.	Planificado
A.6.1.2	Segregación de deberes	SÍ	Asignación de	Cualquier actividad que	Planificado

			responsabilidades relativas a la seguridad de la información	incluya información sensible es aprobada por una persona e implementada por otra. Donde se definirán claramente las responsabilidades y deberes relativos a la seguridad de la información.	
A.6.1.3	Contacto con autoridades	SÍ	Contacto con las autoridades	Se deben mantener los contactos adecuados con las autoridades competentes de la institución, tomando en cuenta las estrategias de continuidad del negocio y el plan de respuesta ante incidentes.	Planificado
A.6.1.4	Contacto con grupos de interés especial	SÍ	Contacto con grupos de especial interés	El jefe de Ceopol es el responsable de supervisar (detallar los nombres de grupos de interés y foros de seguridad), donde se mantendrán los contactos adecuados con grupos de interés especial u otros, asociaciones profesionales especializadas en seguridad.	Planificado

A.6.1.4	Seguridad de la información en gestión de proyectos	SÍ	Ordenadores portátiles, comunicaciones móviles y teletrabajo	El gerente de proyecto debe incluir las reglas correspondientes sobre seguridad de la información en cada proyecto, así como las acciones y tareas a cumplir que le sean asignadas a cada integrante del grupo.	Planificado
A.6.2	Dispositivos móviles y teletrabajo	SÍ	Ordenadores portátiles, comunicaciones móviles y teletrabajo	Se implantará una política formal, adoptando las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de ordenadores portátiles y dispositivos móviles.	Planificado
A.6.2.1	Política sobre dispositivos móviles	SÍ	Ordenadores portátiles y comunicaciones móviles	El equipamiento puede ser llevado fuera de las instalaciones solamente en caso sea requerido, pero no se podrá filtrar ni copiar ninguna información que salga de los sistemas de información de la institución, así como el uso de tarjetas de memoria, medios	Planificado

				de transferencia de datos.	
A.6.2.2	Teletrabajo	SÍ	Teletrabajo	Se redactará e implementará una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondiente.	Planificado

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL

En adelante se recogen las funciones y obligaciones, para el personal policial de la Ceopol con acceso a los sistemas de información de la institución policial. Así como la previa definición de las funciones y obligaciones del personal, teniendo como objeto:

- Proteger los sistemas de información, así como las redes de comunicación propiedad de la institución o bajo su responsabilidad, contra el acceso o uso que no sea autorizado, así como la alteración indebida, destrucción o mal uso.
- Proteger la información perteneciente o proporcionada a la organización en contra de revelaciones no autorizadas o de modo accidental.

A efecto de dar cumplimiento con estas obligaciones independientemente de la función que desempeña o responsabilidades que tiene, la institución exige un carácter general a cualquier empleado o efectivo el cumplimiento de los siguientes aspectos:

- Confidencialidad de la información
- Propiedad intelectual
- Control de acceso físico
- Salidas y entradas de información
- Incidencias
- Uso apropiado de los recursos
- Software
- Hardware
- Conectividad a la red de internet

4.1. Confidencialidad de la información

a. Se debe proteger la información propia o confiada de la institución evitando el uso indebido o su envío no autorizado al exterior a través de cualquier medio de comunicación.
b. Se deberá guardar máxima reserva, por un tiempo indefinido, la información, documentos, claves, análisis, programas y el resto de información a la cual se tenga acceso dentro de la institución policial.

c. En caso de manejar información confidencial, en cualquier tipo de soporte, se deberá entender que la posesión de la misma es temporal, con una obligación de secreto por parte del personal y sin que ello le considere derecho alguno de posesión, titularidad o copia de la misma, inmediatamente después de haber realizado y finalizado las tareas que se hubieran originado, esta debería devolverse a la institución.

4.2. Propiedad intelectual

Queda totalmente prohibido en los sistemas de información de la institución:

a. El uso de aplicaciones informáticas sin la correspondiente licencia. Así como los programas informáticos propiedad de la institución, están protegidos por la propiedad intelectual por lo tanto queda rotundamente prohibida su reproducción, modificación, cesión o comunicación sin ninguna autorización previa.
b. El uso, reproducción, modificación, cesión o comunicación de cualquier otro tipo de obra protegida por la propiedad intelectual sin la debida autorización correspondiente.

4.3. Control de acceso físico

a. Las normas orientadas al acceso físico de las instalaciones de la Ceopol que albergan los sistemas de información y los locales de tratamiento son los siguientes:
b. El acceso a las instalaciones de la institución donde se encuentran los sistemas de información y locales de tratamiento, será realizado previo paso por un sistema de control de acceso físico o con la autorización del responsable(s) de las instalaciones de la institución.

4.4. Salidas y entradas de información

a. Todo tipo de salida y entrada de información de la institución sea esta de carácter personal, deberá ser realizada por el personal autorizado y será necesaria la autorización formal del responsable del fichero de donde provienen los datos.
b. Para la salida de la información de alto nivel confidencial, se deberán cifrar los mismos o utilizar cualquier otro mecanismo que no permitan el acceso o su manipulación durante el transporte.

4.5. Incidencias

a. El personal de la organización y de terceras partes, tiene como obligación la comunicación de cualquier incidencia que se pueda producir la cual esté relacionada con los sistemas de información o de cualquier otro recurso informático de la institución.
b. La comunicación, gestión y resolución de las incidencias de seguridad se realizarán mediante el sistema de gestión de incidencias es cual es habilitado por la institución.

4.6. Uso apropiado de los recursos informáticos

Los recursos informáticos ofrecidos por la institución (datos, software, comunicaciones, etc.), están disponibles exclusivamente para cumplir con las obligaciones labores y con una finalidad corporativa. Por lo que queda terminantemente prohibido cualquier uso distinto del indicado, algunos ejemplos:

a. El uso de los recursos de la institución, así como los que están bajo su supervisión para actividades no relacionadas con la finalidad de la institución.
b. El uso de los equipos, dispositivos o aplicaciones los cuales no estén especificados como parte de software y/o hardware contenidos en la institución.
c. Introducir en los sistemas de información o red corporativa contenidos ilegales, inmorales u ofensivos y en general, sin utilidad alguna en los procesos del negocio de la institución policial.
d. Introducir voluntariamente programas, virus, spyware o cualquier otro software malicioso que sean susceptibles de causar alteraciones en los recursos informáticos de la institución hacia terceros.
e. Desactivar o inutilizar los programas antivirus y de protección de los equipos y sus actualizaciones.
f. Intentar eliminar, modificar, inutilizar los datos, programas o cualquier otra información propios de la institución.
g. Conectarse a la red corporativa a través de otros medios que no sean los definidos y administrados por la institución.
h. Intentar descubrir o descifrar las claves de acceso o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la institución policial.

4.7. Uso apropiado de los recursos y sistemas operativos

a. Los usuarios deben utilizar únicamente las versiones de software facilitadas por la institución y así seguir las normas de utilización.
b. La oficina de Tecnologías de la Información y Comunicación de la Región Policial Junín, es el responsable de definir los programas de uso estandarizado en la institución y de realizar las instalaciones en los PCs.
c. Los usuarios no deben instalar ni borrar ningún tipo de programa informático en su PC.

4.8. Hardware

a. El personal en su actividad laboral, deben hacer uso únicamente del hardware instalado en los equipos propiedad de la institución y cuya función lo requiere para el trabajo que desempeña.
b. El personal en ningún caso accederá físicamente al interior del equipo que tiene asignado para su trabajo o que pertenezca a la propiedad de la institución. En caso necesario se comunicará la incidencia, según el protocolo habilitado, para que el departamento indicado o en su defecto

el encargado de su función, realice las tareas de reparación, instalación o mantenimiento.

c. Los usuarios no manipularán los mecanismos de seguridad que la organización implemente en los dispositivos (equipos, portátiles, móviles, etc.)
d. No sacar equipos, dispositivos o soportes de las instalaciones sin la autorización necesaria, y en todo caso, con los controles y medidas que se hayan establecido para cada supuesto.

4.9. Conectividad a la red de Internet

Las normas referentes al correo electrónico son:

a. El servicio de correo electrónico que la organización pone a disposición de los usuarios tiene un uso estrictamente profesional y destinado a cubrir las necesidades del puesto.
b. Queda terminantemente prohibido intentar leer, copiar o borrar mensajes de correo electrónico de otros usuarios.
c. El personal no debe enviar mensajes de correo electrónico de manera masiva o de tipo primordial con fines publicitarios o comerciales. En el caso que sea necesario, dada la función del usuario, este tipo de mensajes se gestionará con la dirección de la institución y con el responsable de seguridad.

Central de Operaciones Policiales de la Región Policial Junín

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PLAN DE TRATAMIENTO DE RIESGOS

Versión: 01

Código	**:**	**CPTR**
Fecha	**:**	**16/01/2017**
Creado por	**:**	**Jean Carlo Zacarias Villafranca**
Aprobado por	**:**	**Jefe de Estado Mayor-OFIPLAAD**
Nivel de Confidencialidad	**:**	**Intimo / Intermedio / Superficial**

Para conseguir los objetivos que perseguimos con el SGSI, es necesario e imprescindible ejecutar las siguientes actividades

Actividad	Recursos generales y financieros requeridos	Recursos humanos requeridos	Recursos de capacitación	Control de riesgos (evitar, prevenir y proteger)	Función del riesgo (aceptar, retener o transferir)	Opciones del riesgo
Políticas para seguridad de la información	Documentación en papel o formato digital, recursos asumidos por el Gobierno en el presupuesto asignado a la Unidad Ejecutora N° 10	Personal encargado de gestionar la documentación referente a las políticas de seguridad	Ciclos de capacitación al personal policial, dado por personal experto o especialista en seguridad de la información e informática.	Prevenir	Transferir	Elección de controles
Revisión de las políticas para seguridad de la información	Documentación establecida y finalizada acerca de políticas establecidas anteriormente	Personal policial del Estado Mayor experto en temas de seguridad, con apoyo de personal especializado.	Ciclos de capacitación dirigida al personal policial que interactúa con los sistemas de información.	Proteger	Retener	Evitar el riesgo
Inventario de activos	Inventario de los activos de la institución a cargo de personal de la Unidad Ejecutora N° 10 o personal externo especializado en tema de inventarios.	Personal experto en levantamiento de políticas de la seguridad de la información	Registros para entender mejor las necesidades de seguridad de información y determinar los controles para asegurar la confidencialidad,	Prevenir	Aceptar	Elección de controles

			integridad y disponibilidad de la información			
Mantenimiento de equipo	Recursos del presupuesto alcanzado a Unidad Ejecutora N° 10, destinado para los equipos e infraestructura de la institución policial.	Personal técnico especializado en el área de tecnologías de información e infraestructura de hardware y software.	Mantenimiento para los equipos de la institución policial bajo tres aspectos de capacitación: mantenimiento preventivo, correctivo y predictivo.	Prevenir	Aceptar	Evitar el riesgo
Procedimientos y políticas sobre transferencia de información	Recursos utilizados por la institución policial asignados en el presupuesto del gobierno destinado a las comisarias del departamento	Personal encargado de velar en el cumplimiento de procedimientos y transferencia y registros de información	Cursos y charlas de capacitación orientadas a definir y mejorar procedimientos de manejo de información, así como el uso adecuado de la misma.	Evitar	Retener	Evitar el riesgo
Cumplimiento con las políticas y estándares de seguridad	Recursos utilizados por la institución policial asignados en el presupuesto del Gobierno a la Unidad Ejecutora N° 10	Personal encargado de velar en el cumplimiento de procedimientos y transferencia y registros de información	Cursos y charlas de capacitación orientadas a definir y mejorar procedimientos de manejo de información, así como el uso adecuado de la misma.	Evitar	Retener	Evitar el riesgo

Revisión independiente de la seguridad de la información	Documentación en papel o formato electrónico, Recursos asumidos por el gobierno en el Presupuesto a la Unidad Ejecutora N° 10	Personal encargado de gestionar la documentación referente a las políticas de seguridad	Programas de capacitación al personal efectivo, dado por personal experto en temas de seguridad.	Prevenir	Transferir	Elección de controles
Reporte de debilidades en la seguridad de la información	Documentación establecida y finalizada acerca de políticas establecidas anteriormente	Personal del Estado Mayor experto en temas de seguridad.	Programas de capacitación dirigida a los efectivos de la institución que interactúan con los sistemas de información	Proteger	Retener	Evitar el riesgo
Análisis y especificación de los requerimientos de seguridad de la información	Recursos utilizados por la institución orientados al levantamiento de requisitos de seguridad para la institución policial y próximos a su implantación	Personal experto en toma de requerimientos y necesidades de la institución enfocados a la seguridad en los sistemas de información	Programas de capacitación al personal efectivo, dado por personal experto en temas de seguridad.	Evitar	Aceptar	Elección de controles
Procedimientos documentados de operación	Recursos necesarios apoyados por la Dirección de la Región Policial Junín	Personal policial capacitado en labores de documentación y operación.	Recurso asignado por el Gobierno orientado a brindar capacitación al personal en términos documentarios.	Proteger	Transferir	Elección de controles

Central de Operaciones Policiales de la Región Policial Junín

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PLAN DE INSTRUCCIÓN Y CAPACITACIÓN

Versión: 01

Código	**:**	**CPIC**
Fecha	**:**	**16/12/2016**
Creado por	**:**	**Jean Carlo Zacarias Villafranca**
Aprobado por	**:**	**Jefe de Estado Mayor-OFIPLAAD**
Nivel de Confidencialidad	**:**	**Intimo / Intermedio / Superficial**

REGPOL JUNIN-CEOPOL HYO.
DICIEMBE 2016
HUANCAYO. -

PLAN DE INSTRUCCIÓN N° 001 -2016-DIRNOP/REGPOL-JUNIN/CEOPOL-HYO.

(PARA EJECUTAR CICLO DE CHARLAS PERSONALIZADAS DE INSTRUCCIÓN AL PERSONAL POLICIAL SOBRE POLÍTICAS DE SEGURIDAD DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, DIRIGIDO AL PERSONAL POLICIAL DE LA CENTRAL DE OPERACIONES POLICIALES Y OFICINA REGIONAL DE INTELIGENCIA DE LA REGIÓN POLICIAL JUNÍN)

I. GENERALIDADES

A. OBJETIVO

Establecer normas y procedimientos para impartir conocimientos y procedimientos para la aplicación adecuada del Sistema de Gestión de Seguridad de la Información, dirigido al personal policial de la Central de Operaciones Policiales y Oficina Regional de Inteligencia de la Región Policial Junín.

B. FINALIDAD

a. Unificar criterios para la organización y ejecución del “Ciclo de Charlas teórico-practicas”, relacionados a la aplicación adecuada del Sistema de Gestión de Seguridad de la Información.

b. Orientar al personal policial de la Central de Operaciones Policiales y Oficina Regional de Inteligencia de la Región Policial Junín, el cumplimiento de los dispositivos legales y normas vigentes y la aplicación del Sistema de Gestión de Seguridad de la Información.

c. Establecer los principios ético-profesionales y de disciplina en el comportamiento del personal policial, para lograr exitosamente la implementación del Sistema de Gestión de Seguridad de la Información.

C. ALCANCE

El presente Plan de Instrucción, rige para todo el personal Central de Operaciones Policiales y Oficina Regional de Inteligencia de la Región Policial Junín.

D. BASE LEGAL

a. Constitución Política del Perú.
b. Ley Orgánica de la Policía Nacional del Perú.
c. Ley de creación de la PNP Nº 24949.
d. RM. Nº 1032-90-IN/PNP-DIC90. Reglamento de instrucción del Segundo Nivel de la PNP.
e. Directiva N° 051-DGPNP-EMG-DOPOG-DINST Sobre procedimientos académicos que permita al personal PNP una adecuada instrucción.
f. Ley N° 30096 sobre delitos informáticos Gobierno de la República Peruana.
g. Ley Nº 27806 de Transparencia y Acceso a la Información Pública
h. Resolución Ministerial 004-2016-PCM, aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición.
i. Ley N° 29733 Ley de protección de datos personales 03JUL11.

II. OBJETIVOS

A. GENERAL

1. Lograr que el personal policial de la Central de Operaciones Policiales y Oficina Regional de Inteligencia de la Región Policial Junín, a través del ciclo de charlas personalizadas desarrolladas por Jean Carlo Zacarias Villafranca, sean capacitados en el uso adecuado del Sistema de Gestión de Seguridad de la Información y pleno conocimiento de las Políticas de Seguridad, que conlleven a elevar los niveles de seguridad en el manejo de la información policial para mitigar los riesgos de los activos de información identificados.

2. Reducir las deficiencias en el uso y manejo de la información policial que propician fugas o pérdidas de información.

B. ESPECÍFICO

Lograr que el personal Central de Operaciones Policiales y Oficina Regional de Inteligencia de la Región Policial Junín, adquiera conocimientos, habilidades y destrezas relativos a:

1. La observancia y práctica de normas relacionadas sobre el uso adecuado del Sistema de Gestión de Seguridad de la Información y pleno conocimiento de las Políticas de Seguridad.
2. Instruir al personal PNP. en el empleo de los métodos, técnicas y procedimientos de protección de los activos de la información.

3. Consolidar en los participantes los valores ético-morales que les permita actuar con cautela en sus labores policiales sobre uso y manejo de información policial.
4. Preparar teórica, práctica y psicológicamente al personal policial en su totalidad, para cumplir eficientemente con el uso adecuado de la información policial de carácter secreto, reservado y confidencial.

III. METAS

A. DE ATENCIÓN

El objetivo es capacitar a la totalidad del personal policial, que prestan servicios en la Central de Operaciones Policiales y Oficina Regional de Inteligencia de la Región Policial Junín.

B. DE OCUPACIÓN

La instrucción teórico y práctica estará a cargo de Jean Carlo Zacarias Villafranca, con experiencia académica, especialmente en las políticas y normas de seguridad de la información.

IV. PERFIL EDUCATIVO

A. COMO PERSONA

1. Demostrar equilibrio emocional.
2. Demostrar honestidad, moralidad y ética profesional.
3. Demostrar respeto por la persona humana profesional.
4. Demostrar vocación de servicio, espíritu de equilibrio y justicia.
5. Desarrollar perseverancia y sentido de responsabilidad.
6. Demostrar espíritu de cuerpo y camaradería.

B. COMO CIUDADANO

1. Demostrar respeto por las leyes y normas de cortesía.
2. Demostrar espíritu de solidaridad con sus semejantes.
3. Demostrar capacidad de diálogo y/o comunicación.
4. Demostrar capacidad de convivencia fraterna dentro de la comunidad.

C. COMO PROFESIONAL

1. Los participantes al término del ciclo de charlas del uso adecuado del Sistema de Gestión de Seguridad de la Información, tendrán pleno conocimiento de las Políticas de Seguridad, evitando en el futuro posibles deficiencias en el uso y manejo del Sistema de Gestión de Seguridad de la Información.

2. Dominio y seguridad en su accionar policial, demostrando experiencia, tino y profundo conocimiento de las normas y políticas legales vigentes y de seguridad de los activos de información.

3. Lograr que los participantes se familiaricen y amplíen sus conocimientos en los métodos y técnicas del uso del Sistema de Gestión de Seguridad de la Información.

4. Dominio total del Sistema de Gestión de Seguridad de la Información, con conocimiento de las políticas y normas de seguridad para los activos de la información.

V. ESTRUCTURA CURRICULAR

A. ORGANIZACIÓN CURRICULAR

1. TEMARIO
   a. Definición de información
   b. Definición de un Sistema de Gestión de Seguridad de la Información
   c. La Norma UNE-ISO/IEC 27001:2013
   d. Gestión de riesgos
   e. Políticas de seguridad de la información

2. DISTRIBUCIÓN DEL TIEMPO
   a. El presente ciclo de charlas se ejecutará del 26 al 29DIC16, antes de iniciar al servicio policial (07:45 hrs.)
   b. El tiempo de exposiciones tendrán una duración de 30 minutos.
   c. Asimismo, se realizará una retroalimentación el 30DIC16, de 08:00 a 09:30 hrs.

B. ADMINISTRACIÓN CURRICULAR

METODOLOGÍA DE LA ENSEÑANZA

a. La enseñanza se efectuará mediante charlas por 4 días (26 al 29DIC16) durante 30 minutos y un Taller de retroalimentación que se realizará en única fecha el 30DIC16, por espacio de 1:30 horas.
b. Se ejercitará la capacidad analítica y critica del participante el día de la retroalimentación (30DIC16).
c. Se atenderá por igual las necesidades individuales de los participantes, las consultas se realizarán en cualquier momento del servicio policial.
d. Los conocimientos impartidos se aplicarán a situaciones reales, buscando la participación activa del participante.

VI. RECURSOS

A. FINANCIAMIENTO

Los recursos logísticos serán proporcionados por el S1. PNP Jean Carlo Zacarias Villafranca en coordinación con la Oficina de Telemática de la REGPL Junín.

B. INFRAESTRUCTURA

El presente ciclo de charlas se realizará en las oficinas de la Central de Operaciones Policiales y Oficina Regional de Inteligencia de la Región Policial Junín del 26 al 29DIC16 y en el auditórium de la Región Policial Junín el 30DIC16.

Huancayo, 26 de diciembre del 2016

DISTRIBUCIÓN

-REGPOL JUNIN	01
-ESTADO MAYOR	01
-ARCHIVO	01/03

JMRV/EQC.
jczv.

Vº Bº

_____FDO._____
SA - 31449363 - O+
Jean C. ZACARIAS VILLAFRANCA
S1. PNP

_____FDO._____
OP - 181020
Jesús Moisés RÍOS VIVANCO
GENERAL PNP
DIRECTOR DE LA REGIÓN POLICIAL JUNÍN